software radio and the future of wireless security

michael ossmann
institute for telecommunication sciences

This presentation is an outgrowth of work done under contract to the Institute for Telecommunication Sciences and does not represent the views or policies of the United States federal government.

ITS Institute for Telecommunication Sciences

Boulder, Colorado

ITS Institute for Telecommunication Sciences

U.S. DEPARTMENT OF COMMERCE

NTIA

NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

…te for Telecommunication Sciences

NIST

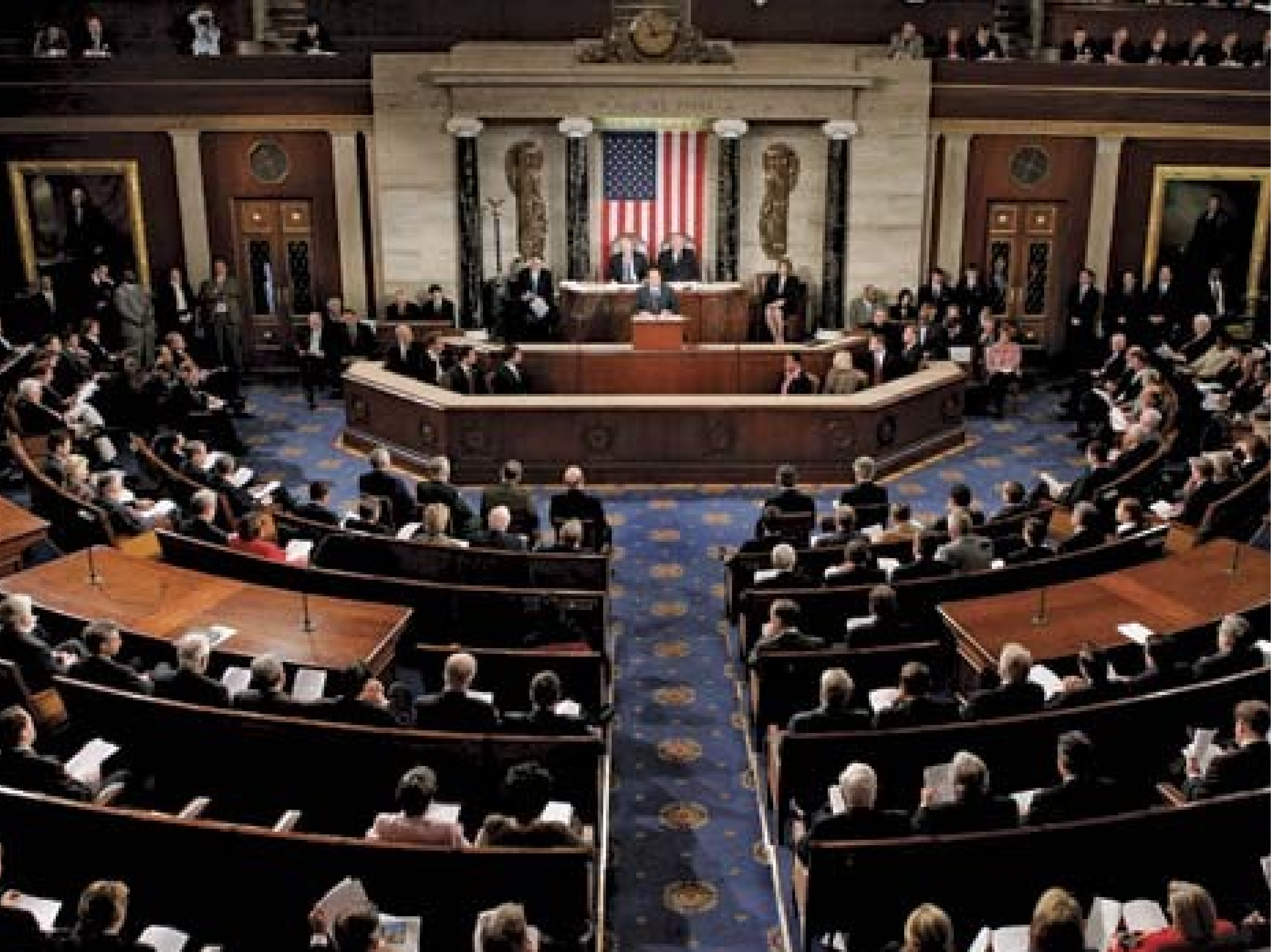
DEPARTMENT OF COMMERCE
★ UNITED STATES OF AMERICA ★

ENT OF COMMERCE
ATIONS & INFORMATION ADMINISTRATION

DEPARTMENT O
UNITED STATES O

U.S. DEPARTMENT OF HOMELAND SECURITY

IONS & INFORMATION ADMINISTRATION




Security
Smart Business.

in the next hour

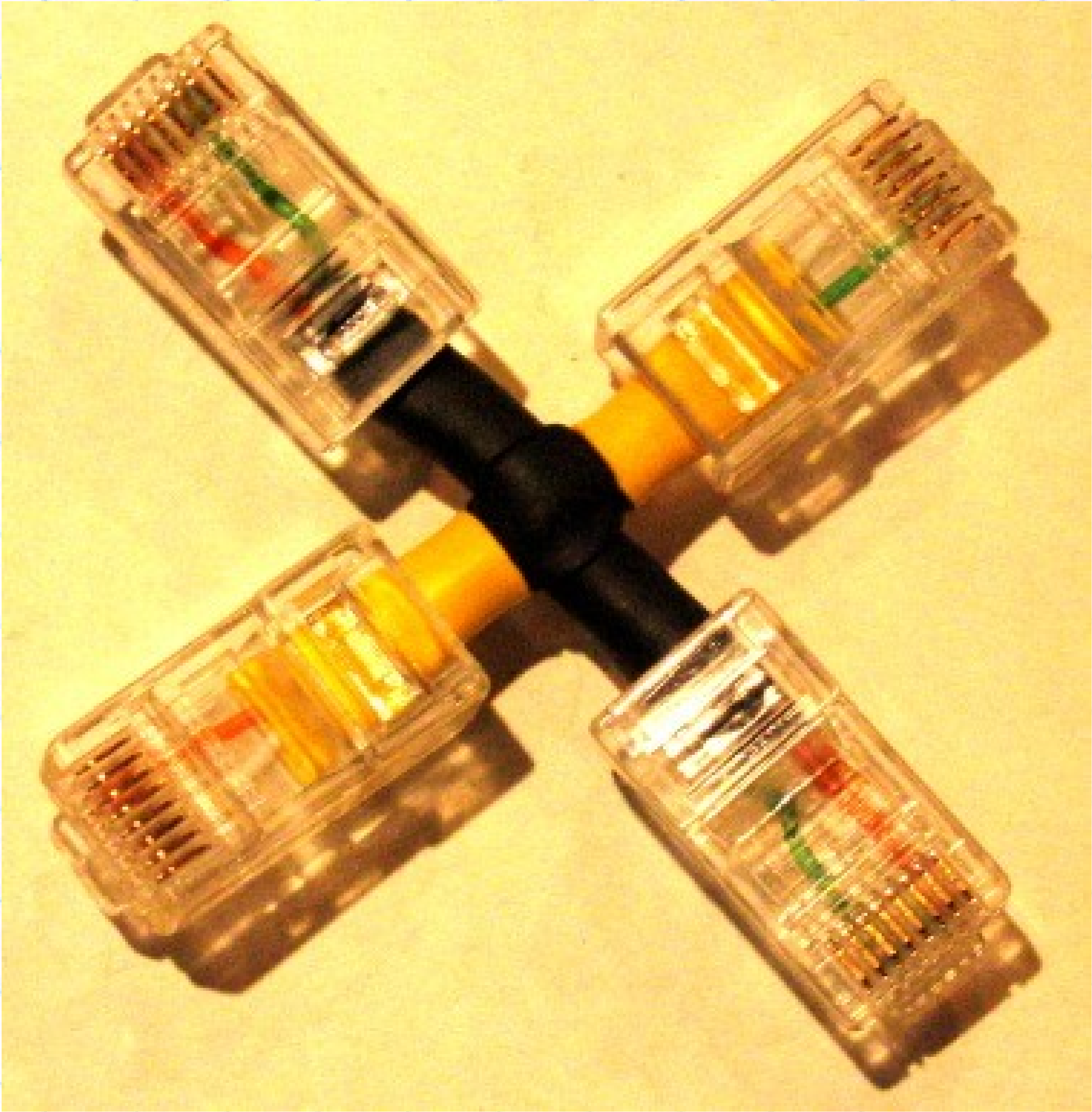
1. software radio
2. global domination
3. security implications
4. demonstration
5. radio for software people

not in the next hour

groundbreaking vulnerabilities

specific wireless protocols


Mystery
Signal
Challenge!



http://ossmann.com/

bh-usa-08/

1. software radio

analog everywhere

sounds

radio waves

tides

heart rhythms

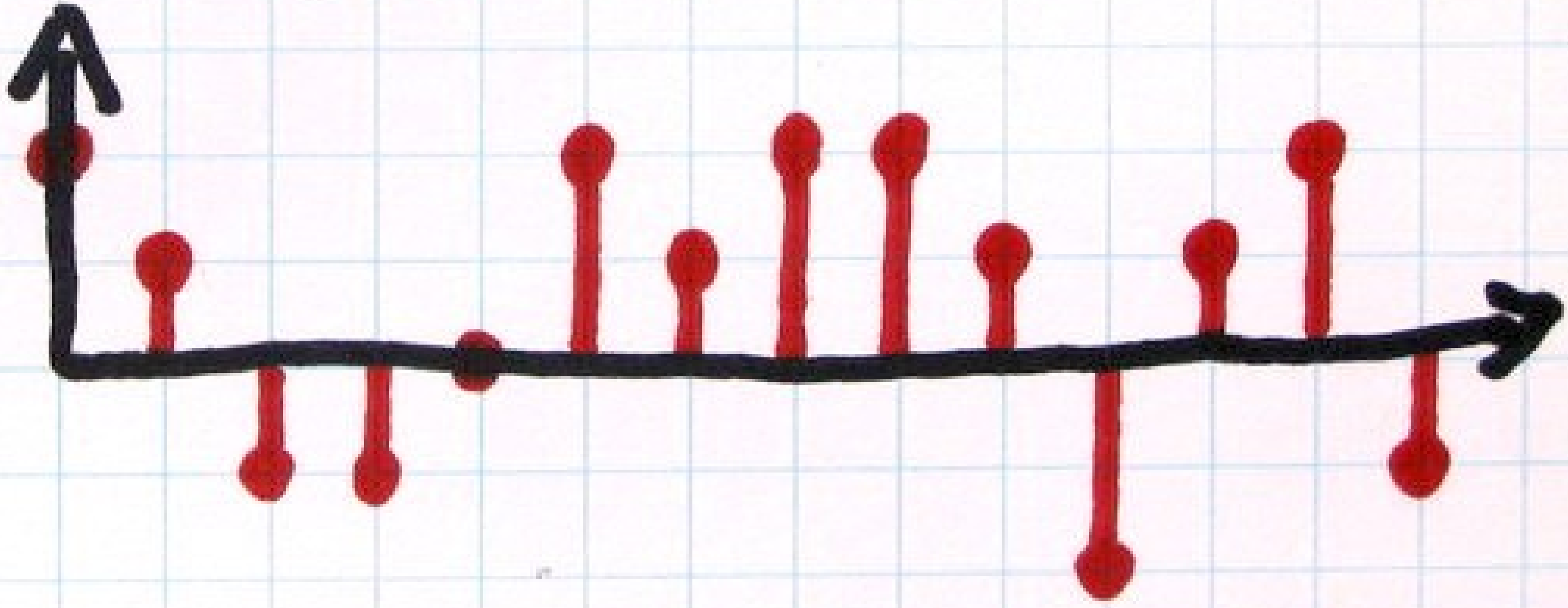
seismic waves

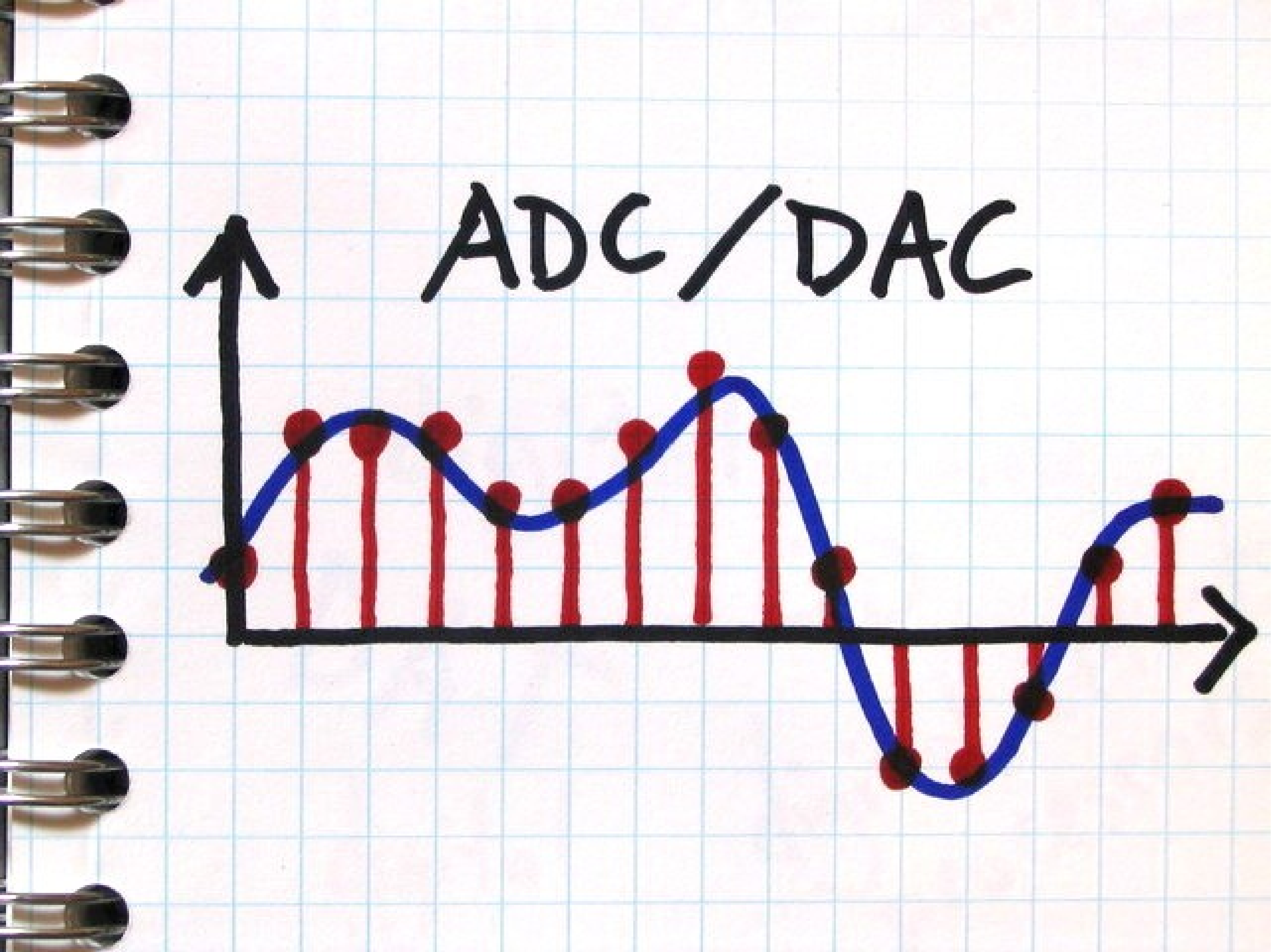
sunspot cycles

images

digital signals

just a sequence of values




ADC / DAC

analog audio

vinyl records

tape

synths

Plain Old
Telephone Service

digital audio

DAT

CD

digital effects processors

digital phone switches

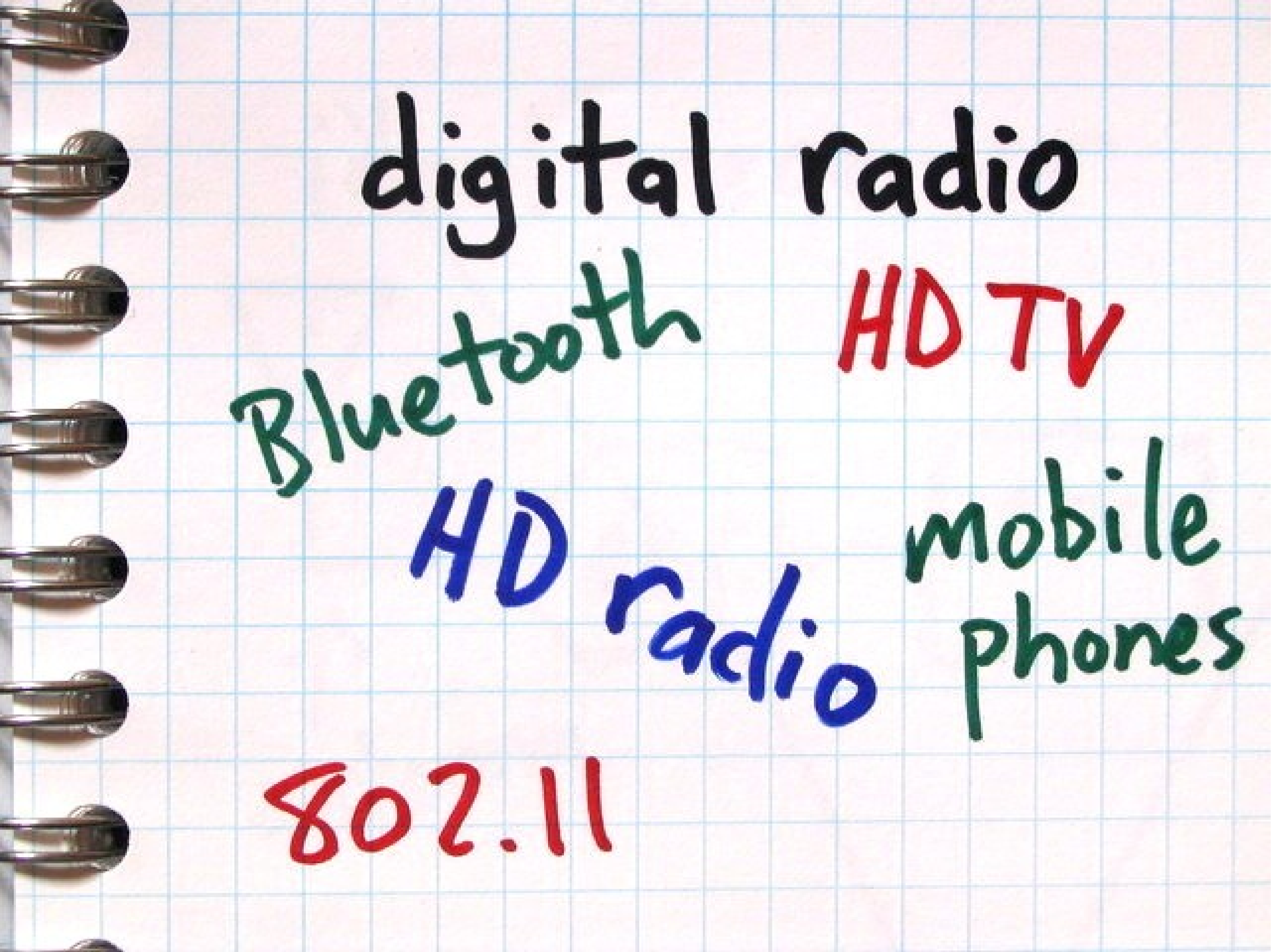
synths


hard disk
recording
MP3
VoIP
explosion!
P2P
Napster
Skype
analog
modeling
synths


software
~~digital~~ audio
revolution

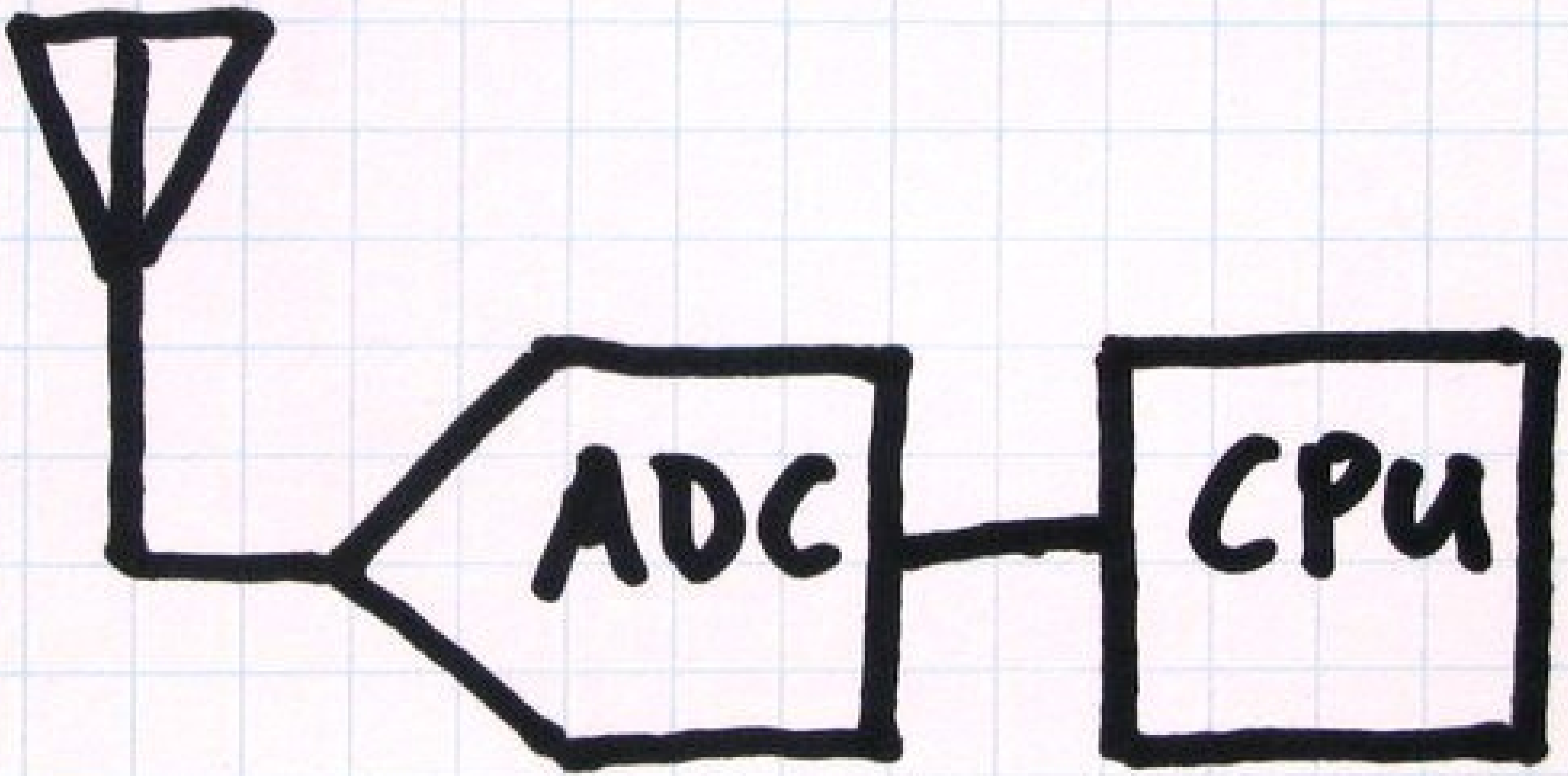
http://ossmann.com/

bh-usa-08/

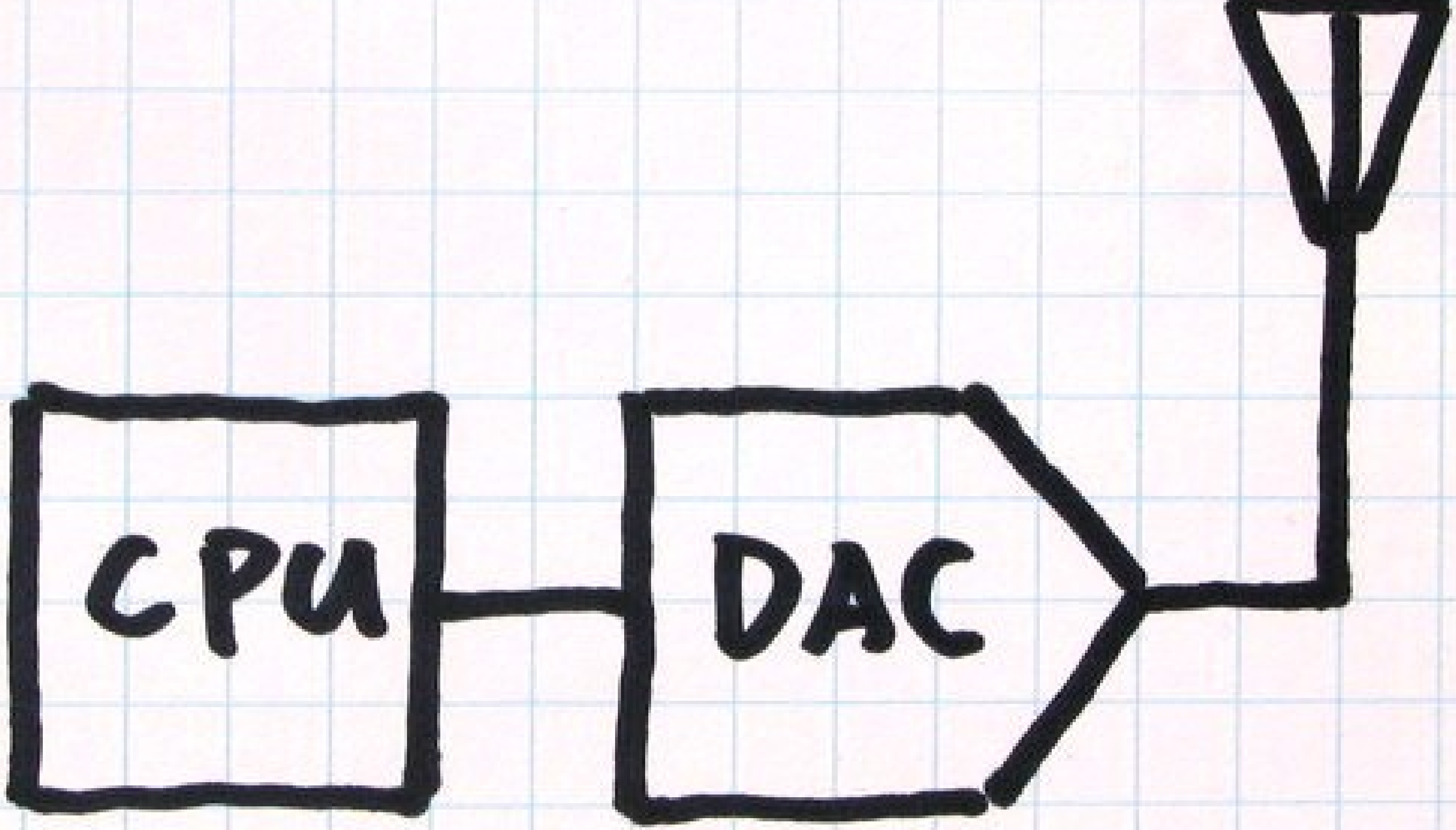

digital radio
Bluetooth
HD TV
HD radio
mobile phones
802.11

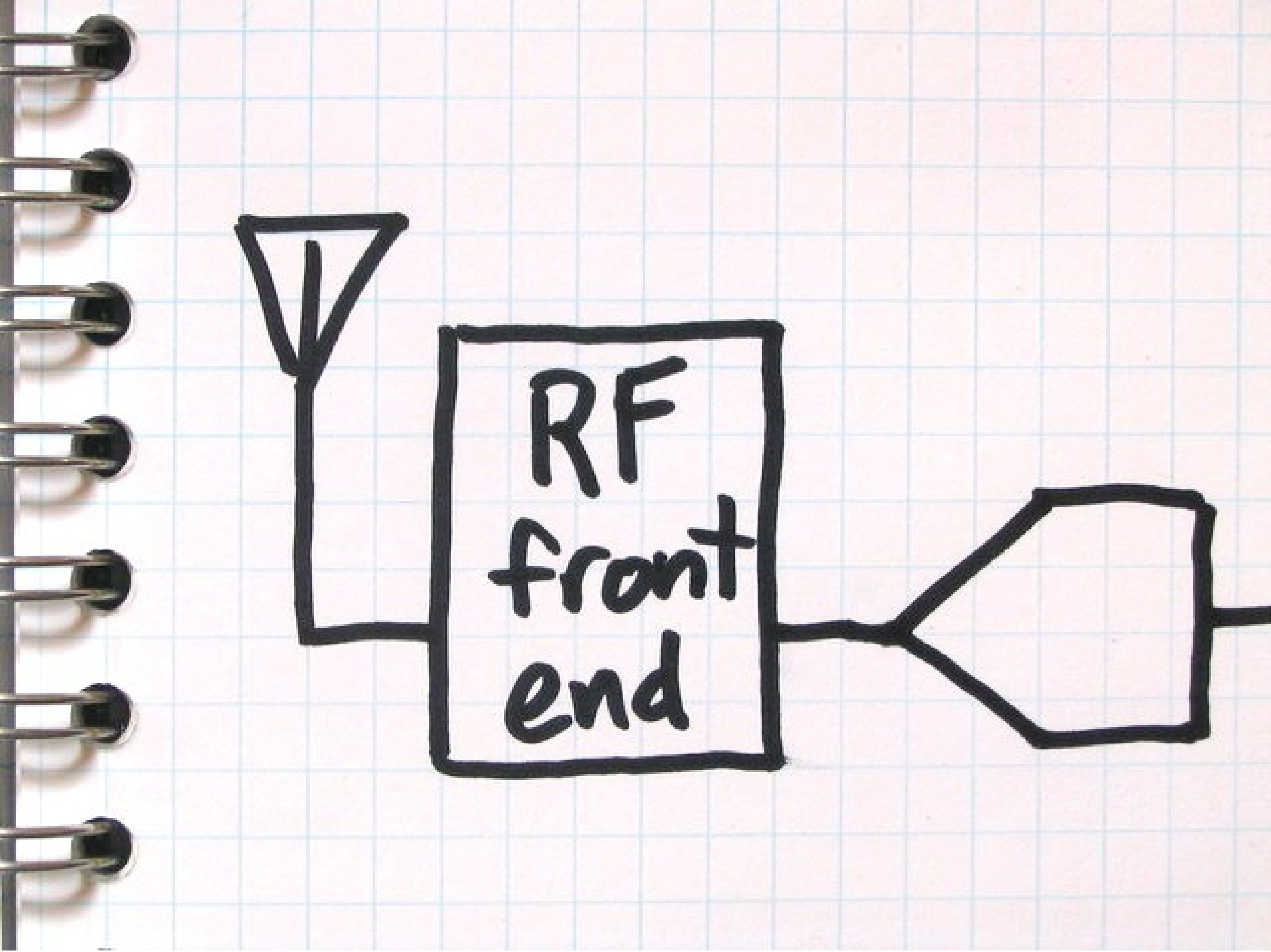
a
signal
is
a
signal

ideal receiver



ideal transmitter




RF
front
end

closed source
software radio

amateur radio gear

WiMAX mobile phones

who knows?

open source
software radio

RF front
ends for
sound cards

USRP

HPSDR

USRP

http://www.ettus.com/

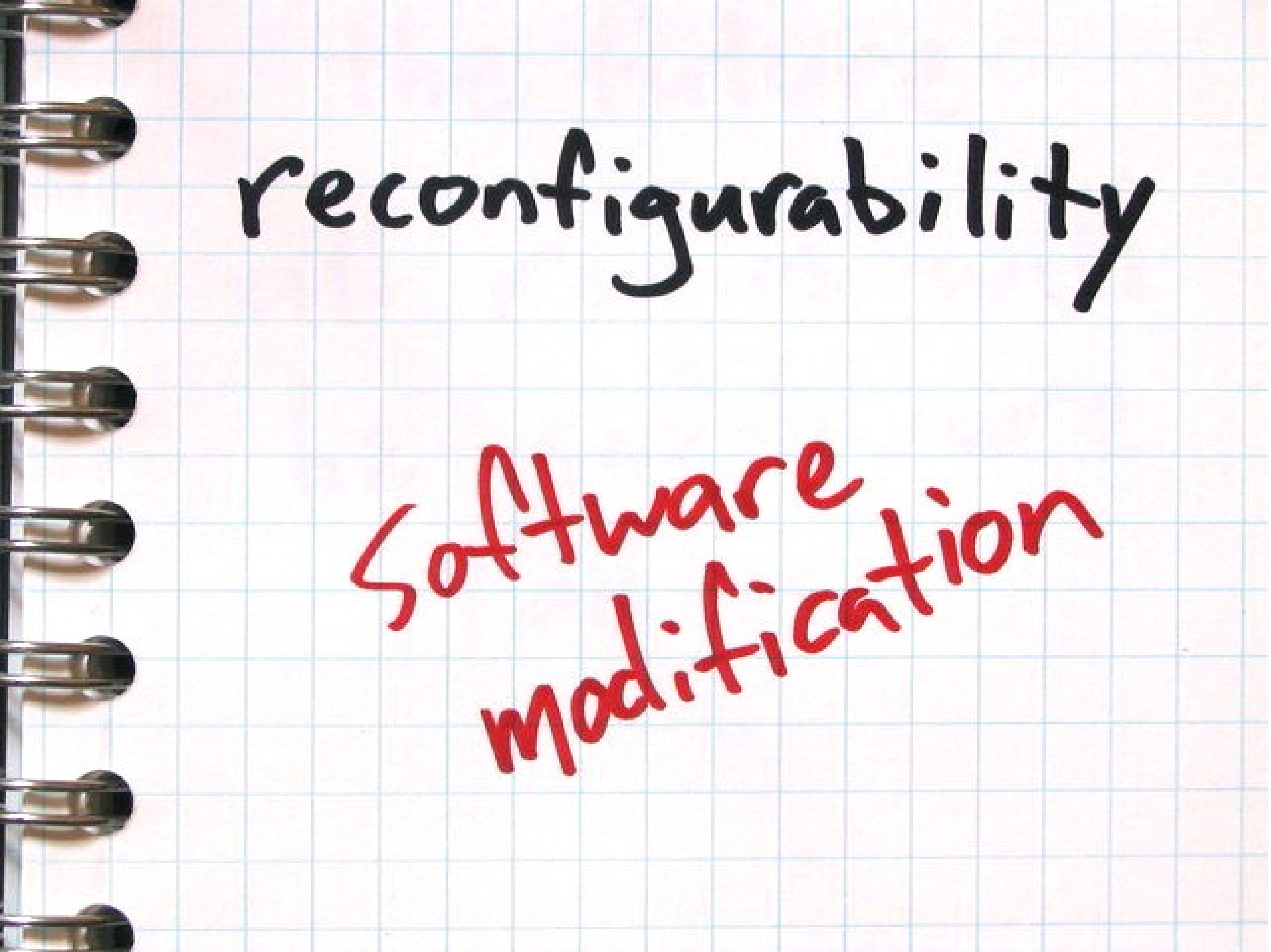
http://ossmann.com/

bh-usa-08/

2. global domination

flexibility

many radios
in one


reconfigurability
Software
modification

cost

high quality
analog
components

or

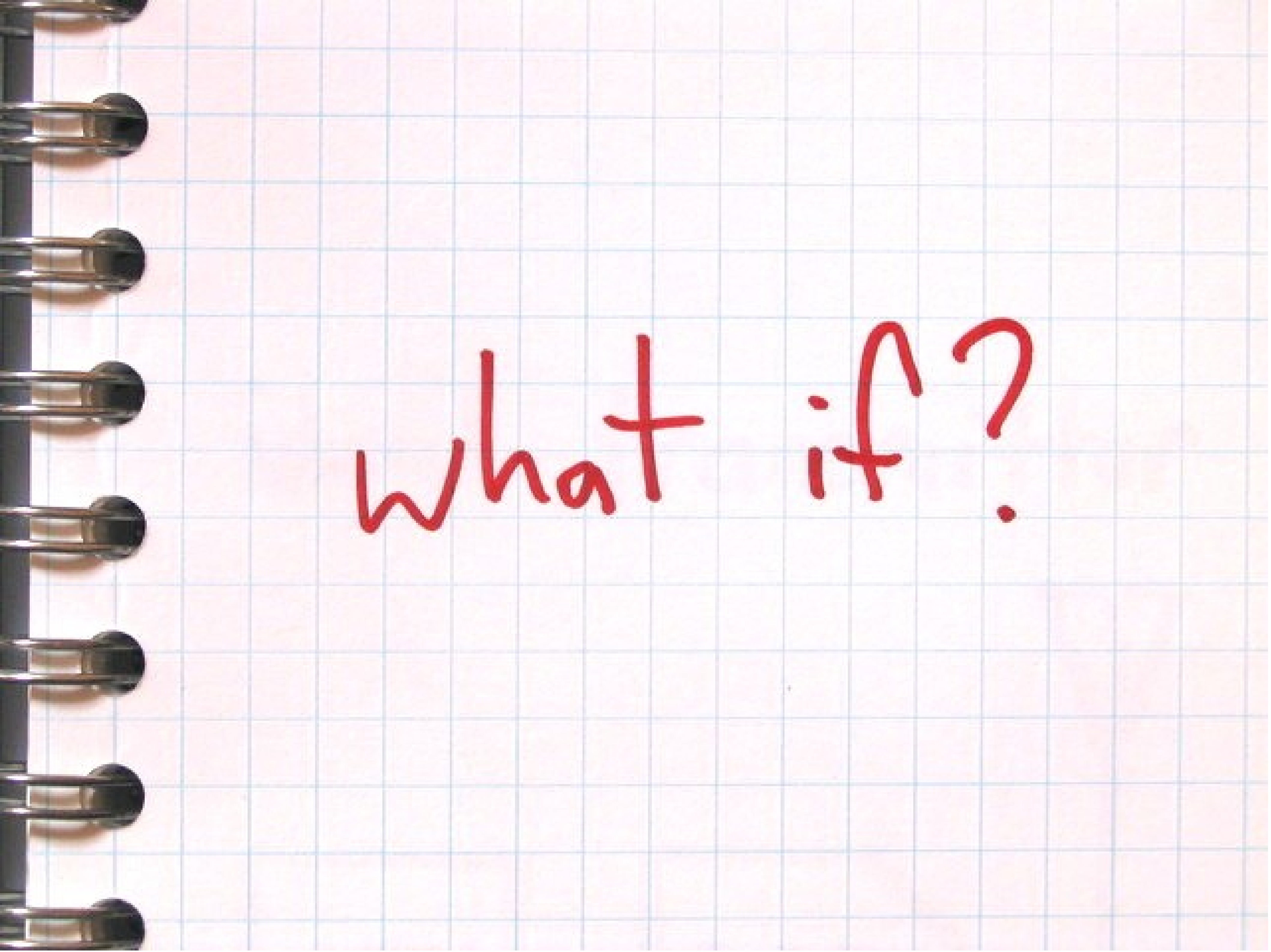
cheap
analog
components
plus
CPU

the future

all radios will be software radios

3. security implications

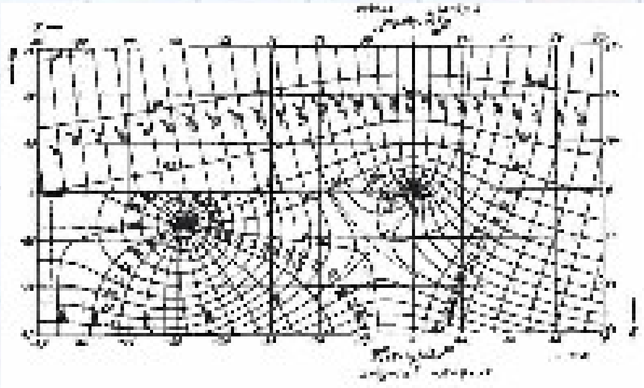
the Wi-Fi lesson


what if?

GSM

http://wiki.thc.org/gsm

USRP



GSM™
The wireless evolution

27 MHz Keyboards

http://remote-exploit.org/

sound card

Bluetooth

http://usenix.org/event/woot07/tech

USRP

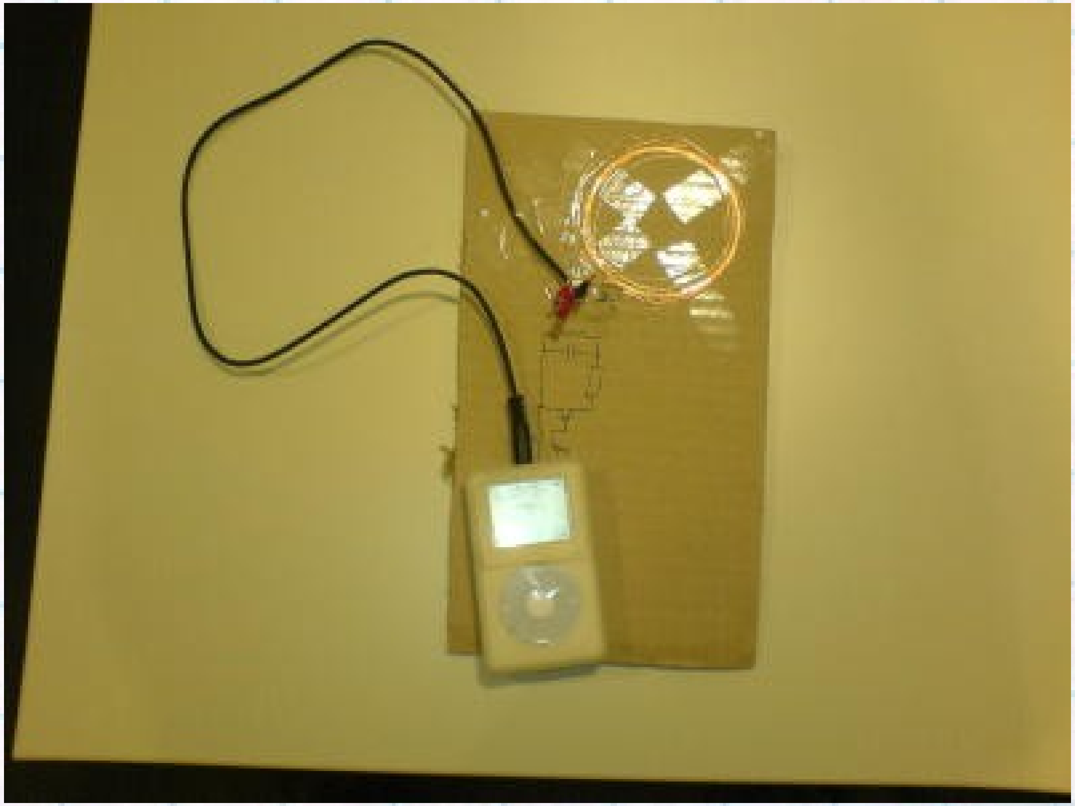
Bluetooth®

RFID

google: ccc 2006 1576

USRP

iPod



mobitex

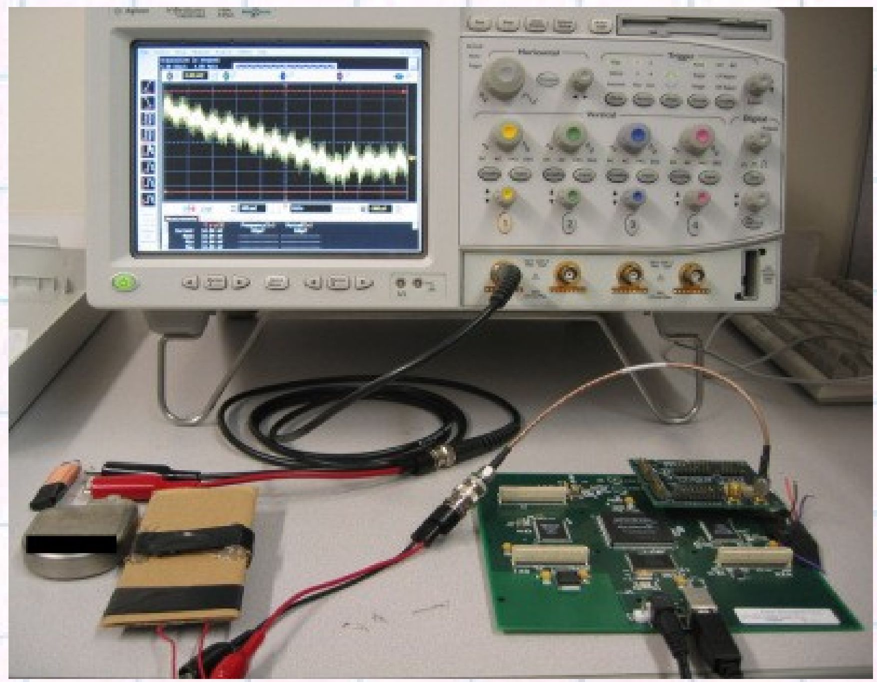
http://toolcrypt.org/

sound card

mobitex
TECHNOLOGY

medical devices

http://secure-medicine.org/



USRP

4. demonstration

5. radio for software people

software radio topics

RF propagation

antennas

ECC

FPGA

calculus

DSP

information theory

abstract algebra

SIMD

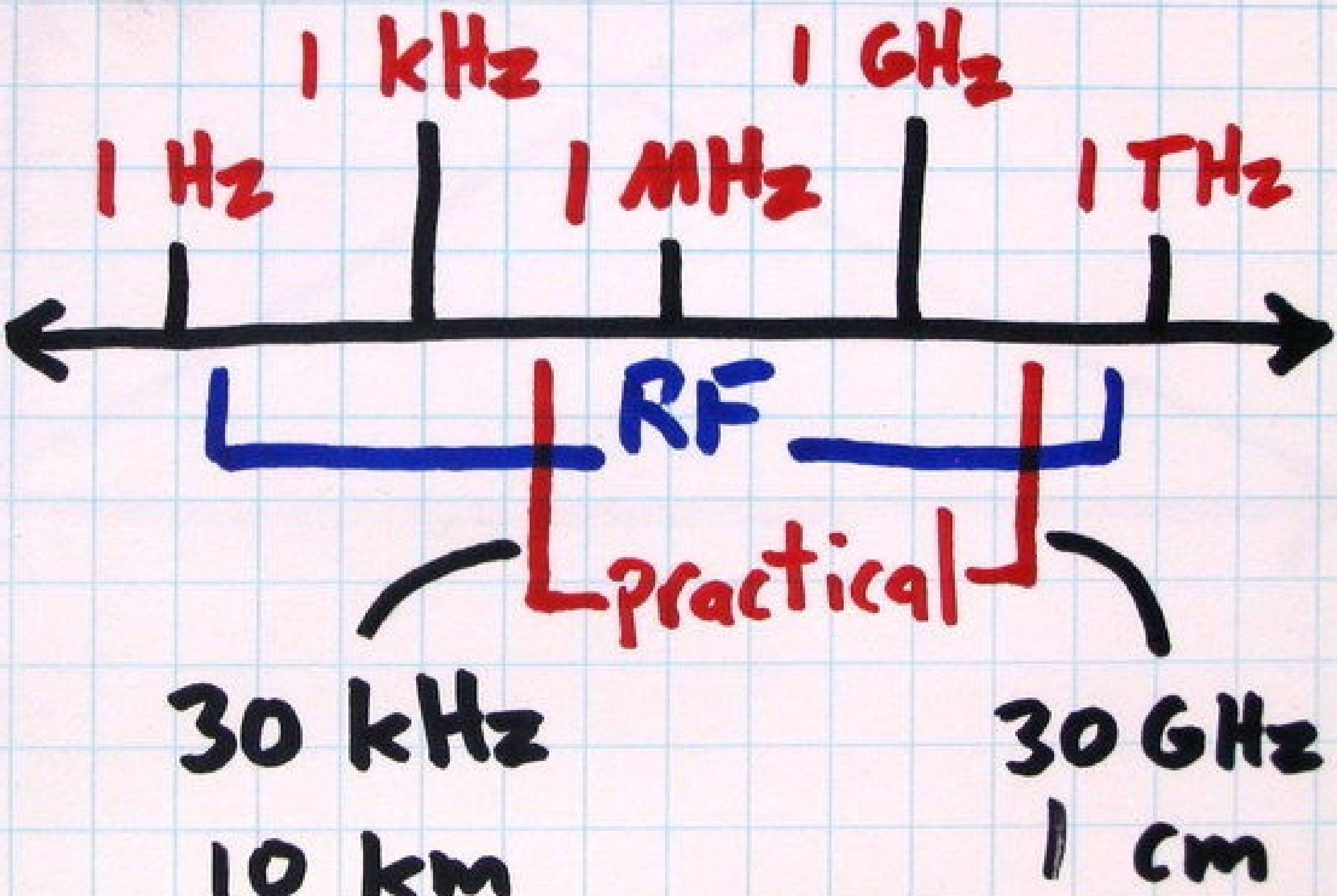
Fourier theory

sampling theory

circuit design

GPU

RF basics

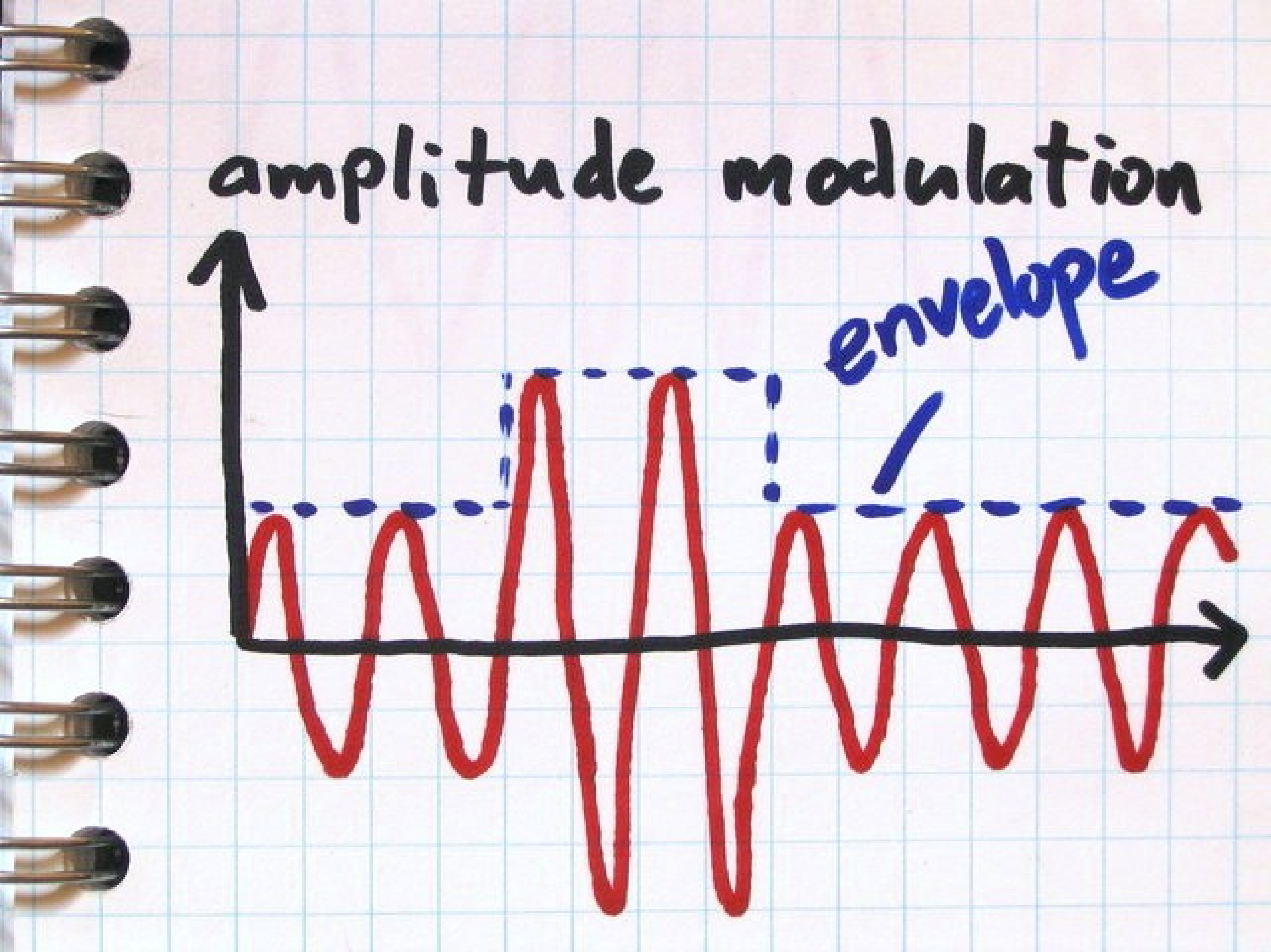


antenna basics

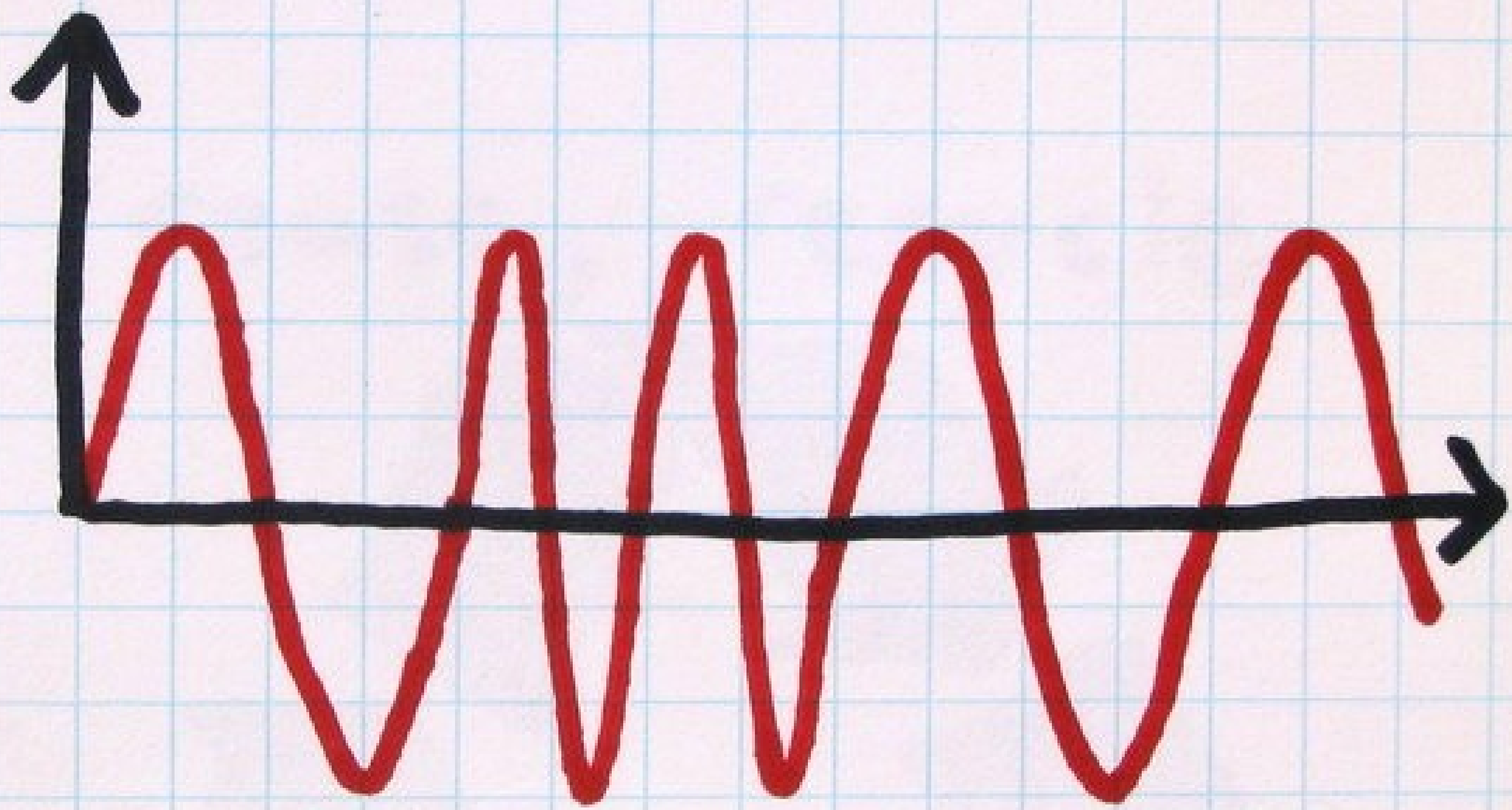
1. proportional to wavelength
2. go big
3. loops for LF

Goldilocks and the Three Bands

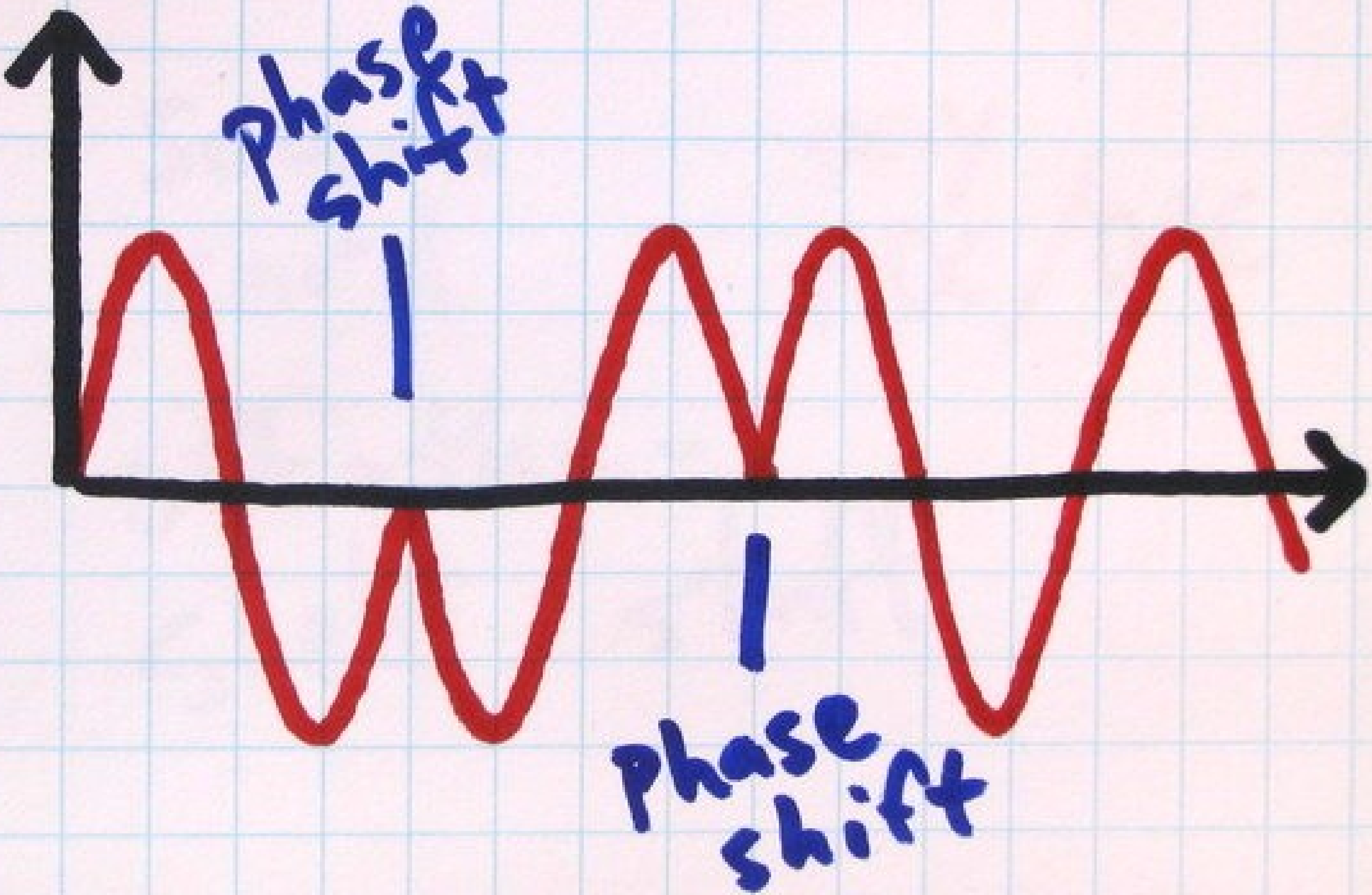
kHz MHz GHz

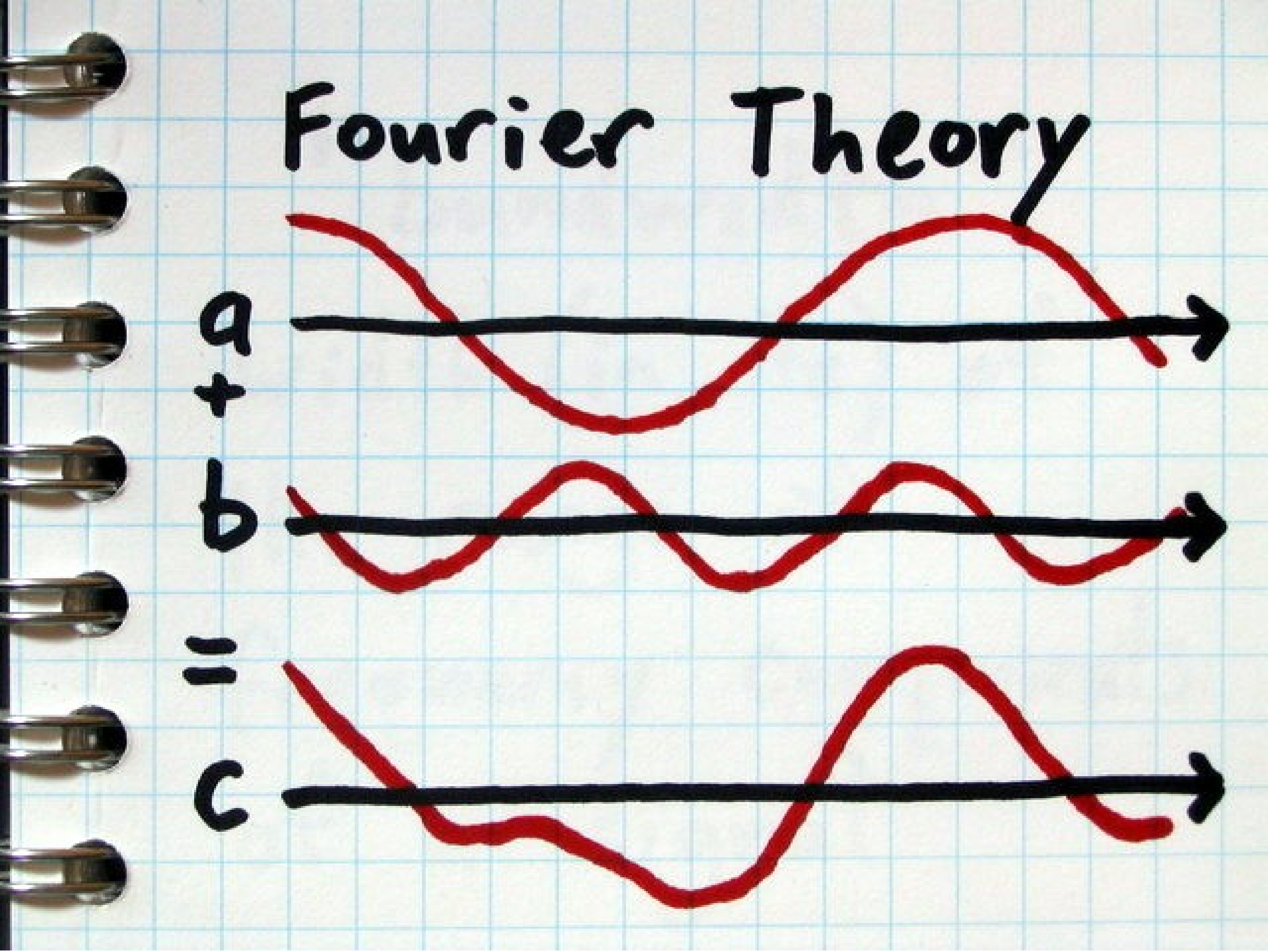

amplitude modulation
envelope

frequency modulation



Phase modulation

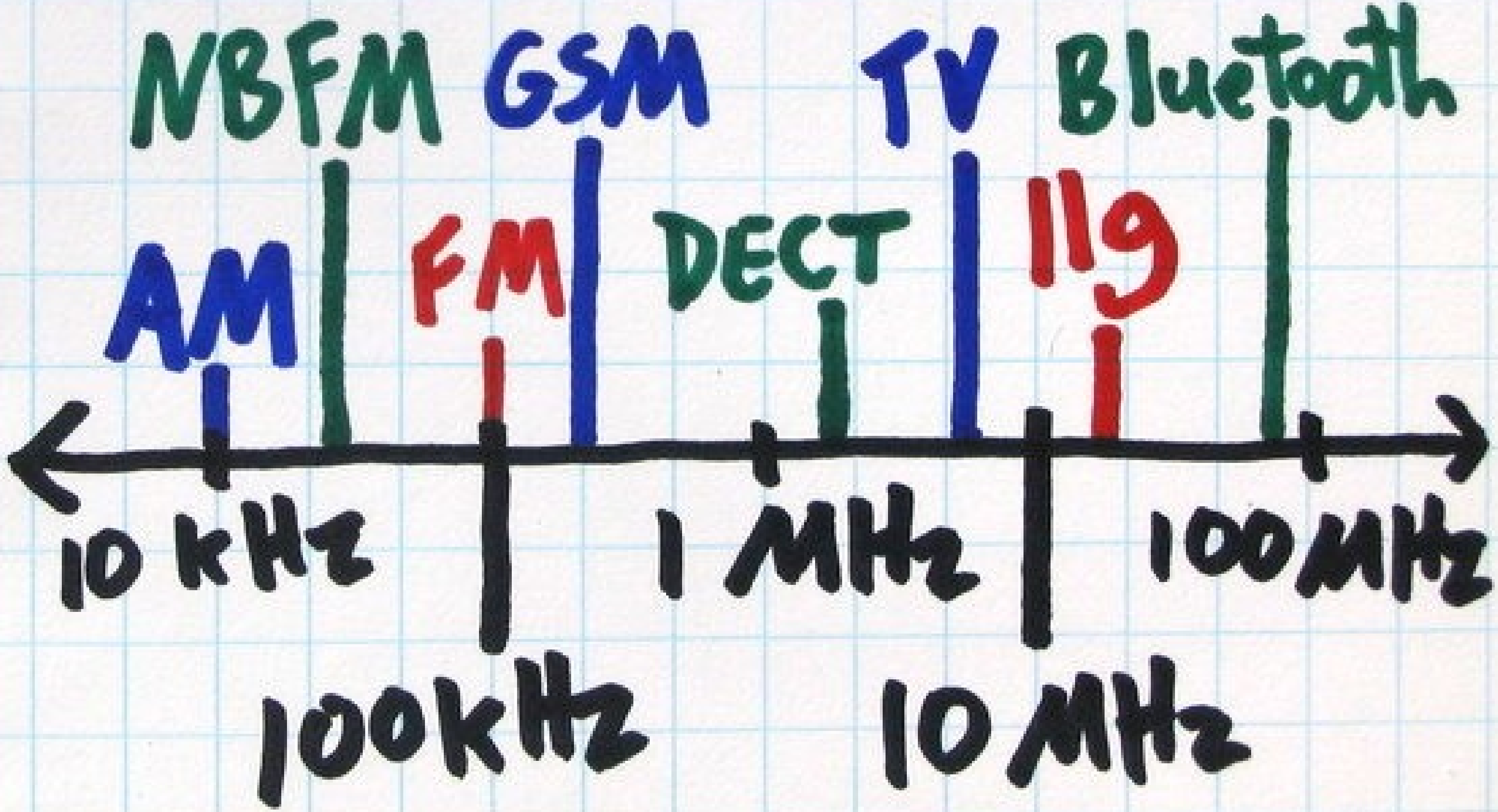



Fourier Theory
a
+
b
=
c

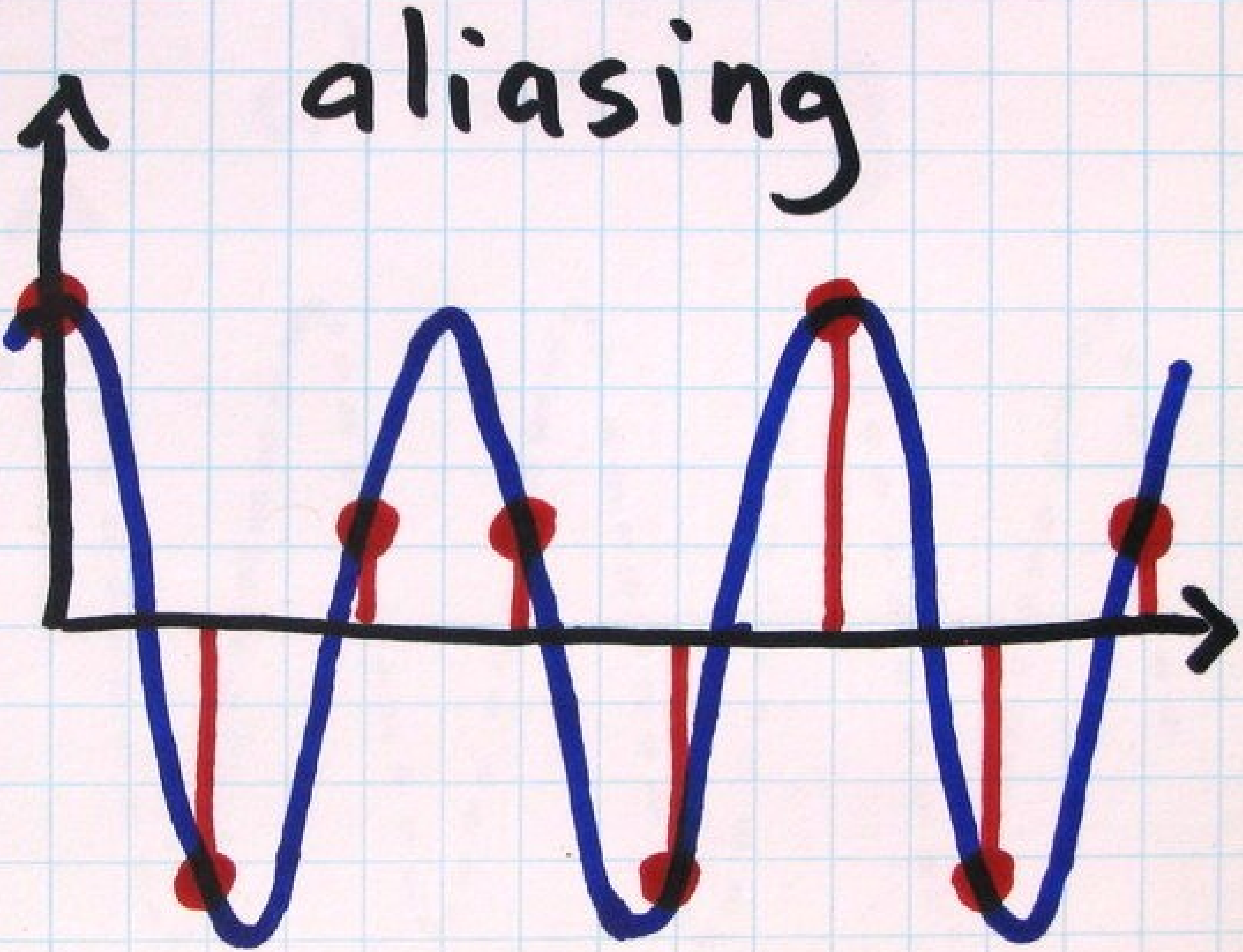
"bandwidth"

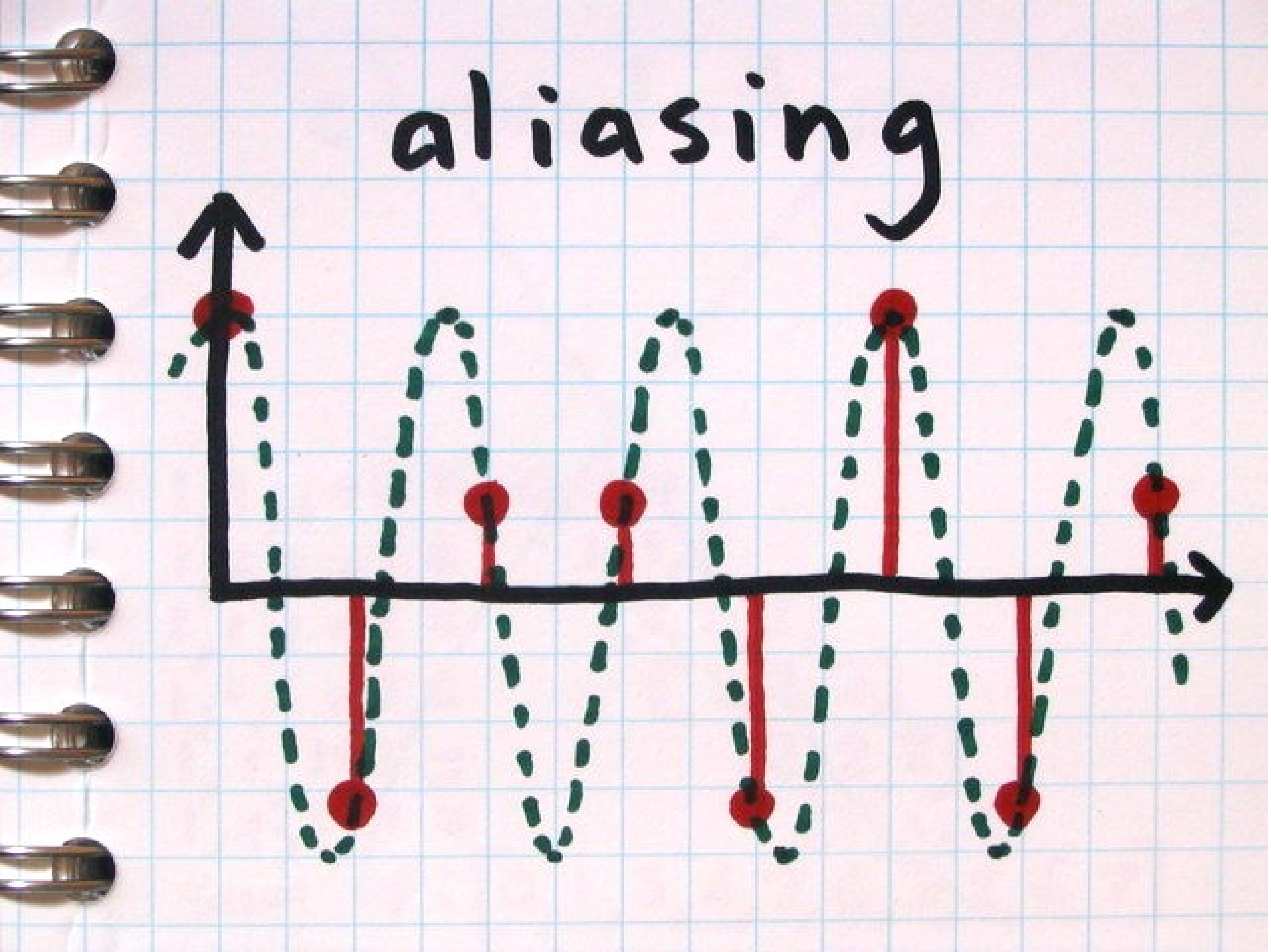
width (in Hz) of
the range of
frequency components
of a signal

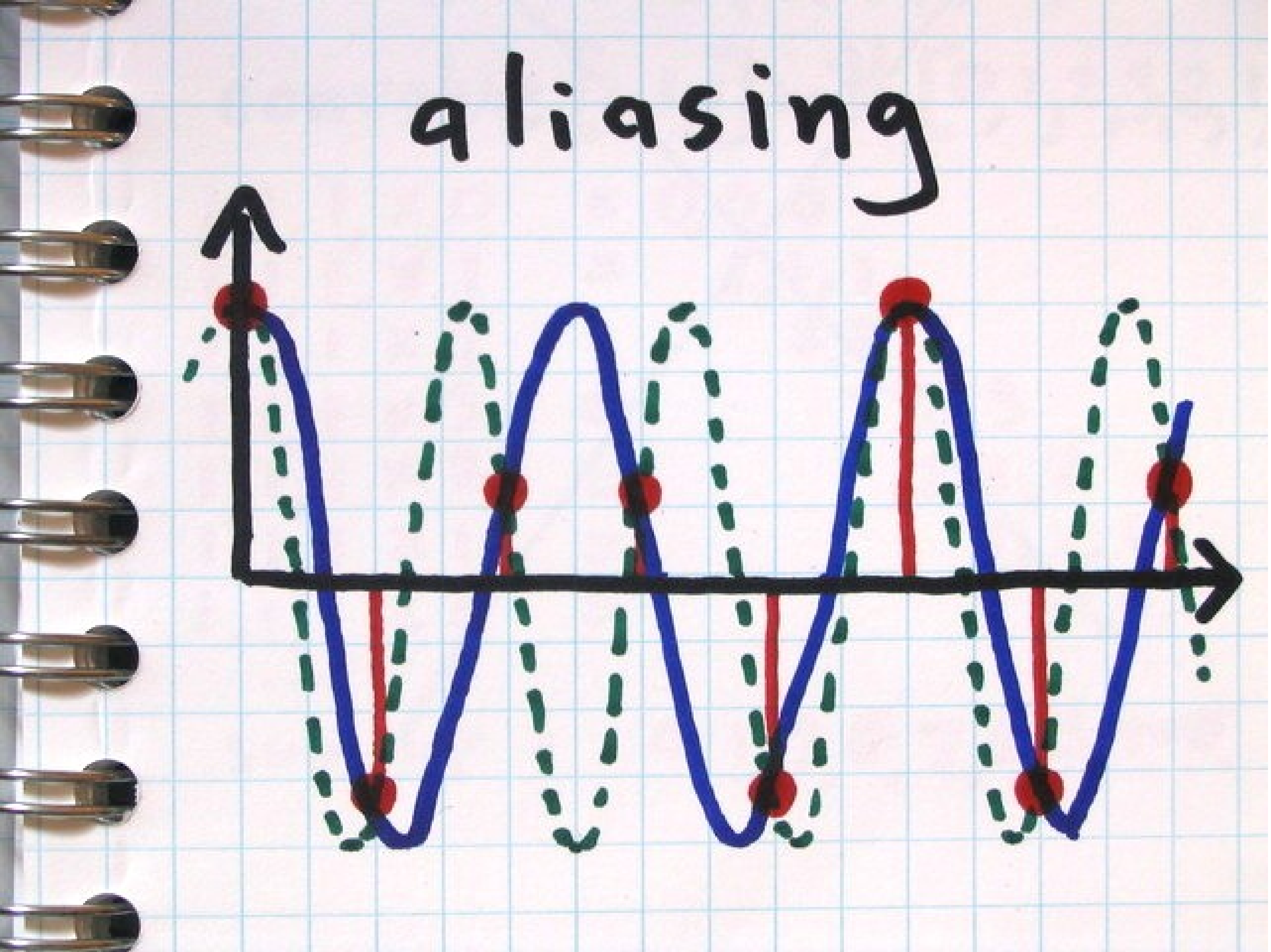
bandwidth



NBFM
GSM
TV
Bluetooth
AM
FM
DECT
11g
10 kHz
1 MHz
100 MHz
100 kHz
10 MHz


aliasing


aliasing


aliasing

sampling

sampling rate > twice bandwidth

hardware

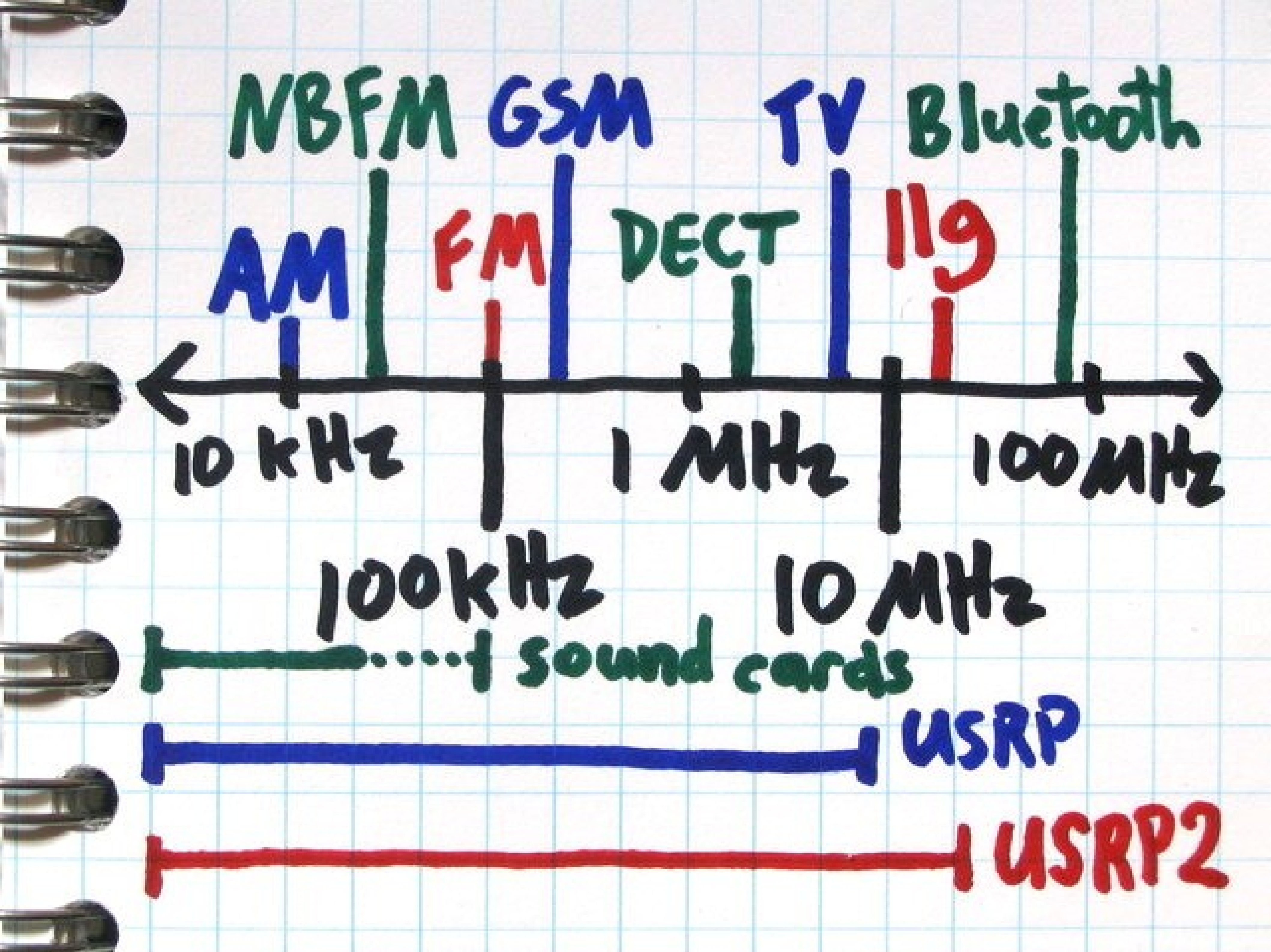
USRP

HPSDR

sound card

any ADC/DAC

off-the-shelf stuff


NBFM
GSM
TV
Bluetooth
AM
FM
DECT
11g
10 kHz
1 MHz
100 MHz
100 kHz
10 MHz
sound cards
USRP
USRP2

convolution

[1, 1, 1] * [0, 1, 2, 3, 2, 1, 0, ...]

1, 1, 1 × 0 = 0, 0, 0

1, 1, 1 × 1 = 1, 1, 1

1, 1, 1 × 2 = 2, 2, 2

1, 1, 1 × 3 = 3, 3, 3

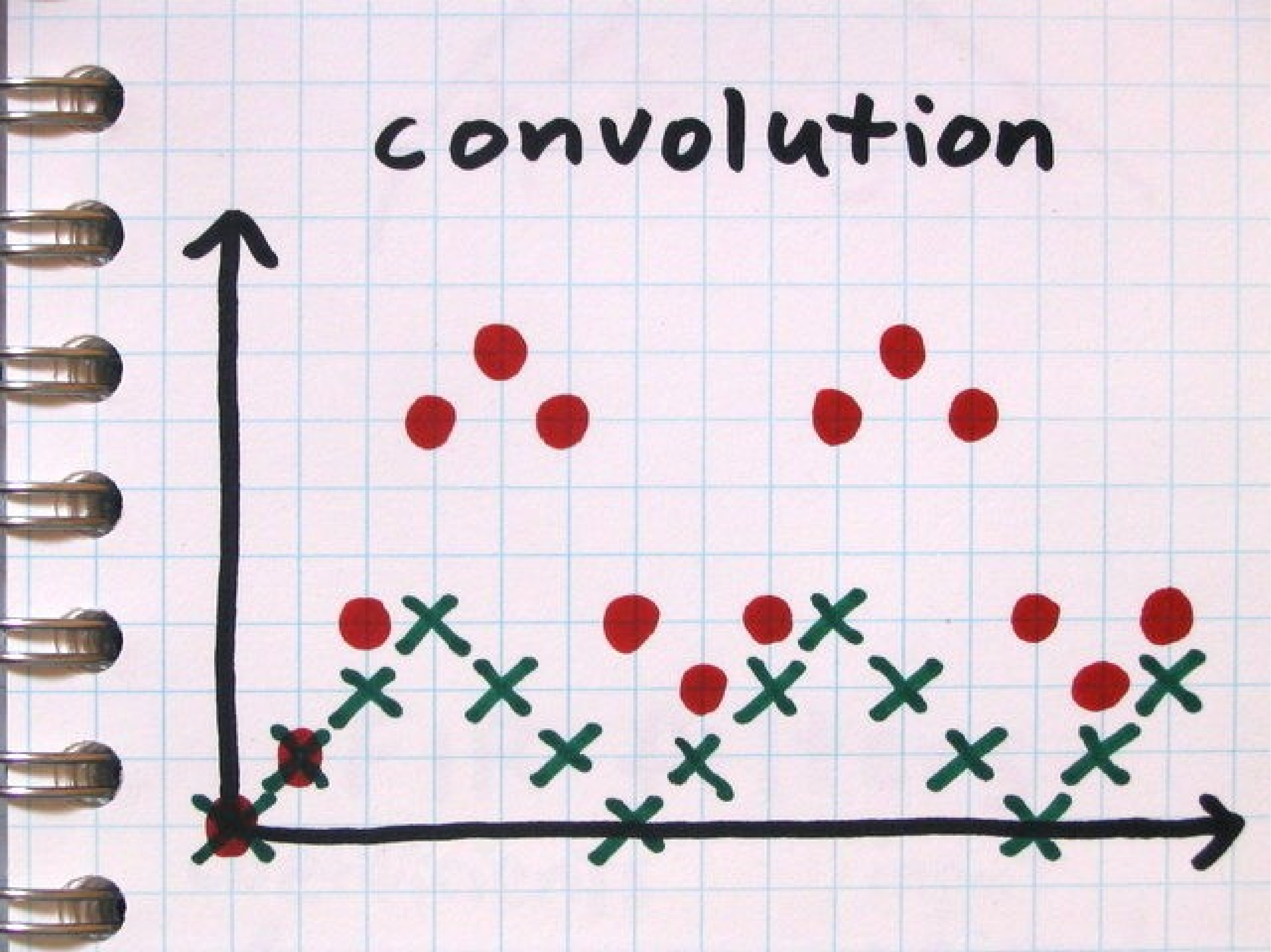
1, 1, 1 × 2 = 2, 2, 2

1, 1, 1 × 1 = 1, 1, 1

1, 1, 1 × 0 = 0, 0, 0

...

sum up : 0, 1, 3, 6, 7, 6, 3, ...


convolution

FIR filters

$$\overbrace{[1,1,1]}^{\text{coefficients}} * \overbrace{[0,1,2,3,2,1,0,\ldots]}^{\text{input signal}}$$

$$= \underbrace{[0,1,3,6,7,6,3,\ldots]}_{\text{output signal}}$$

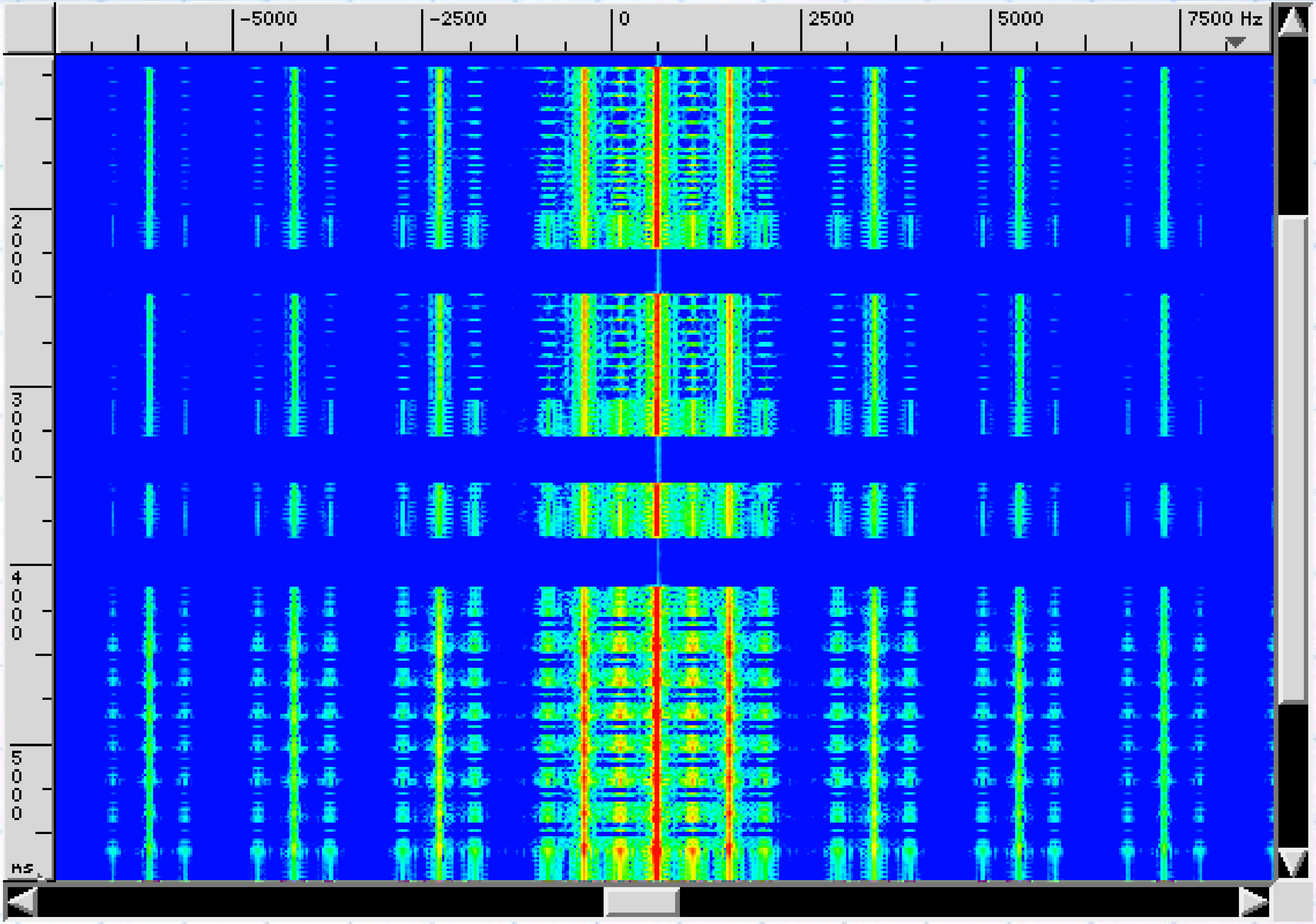
visualize

GNU Radio

MATLAB / Octave

gnuplot

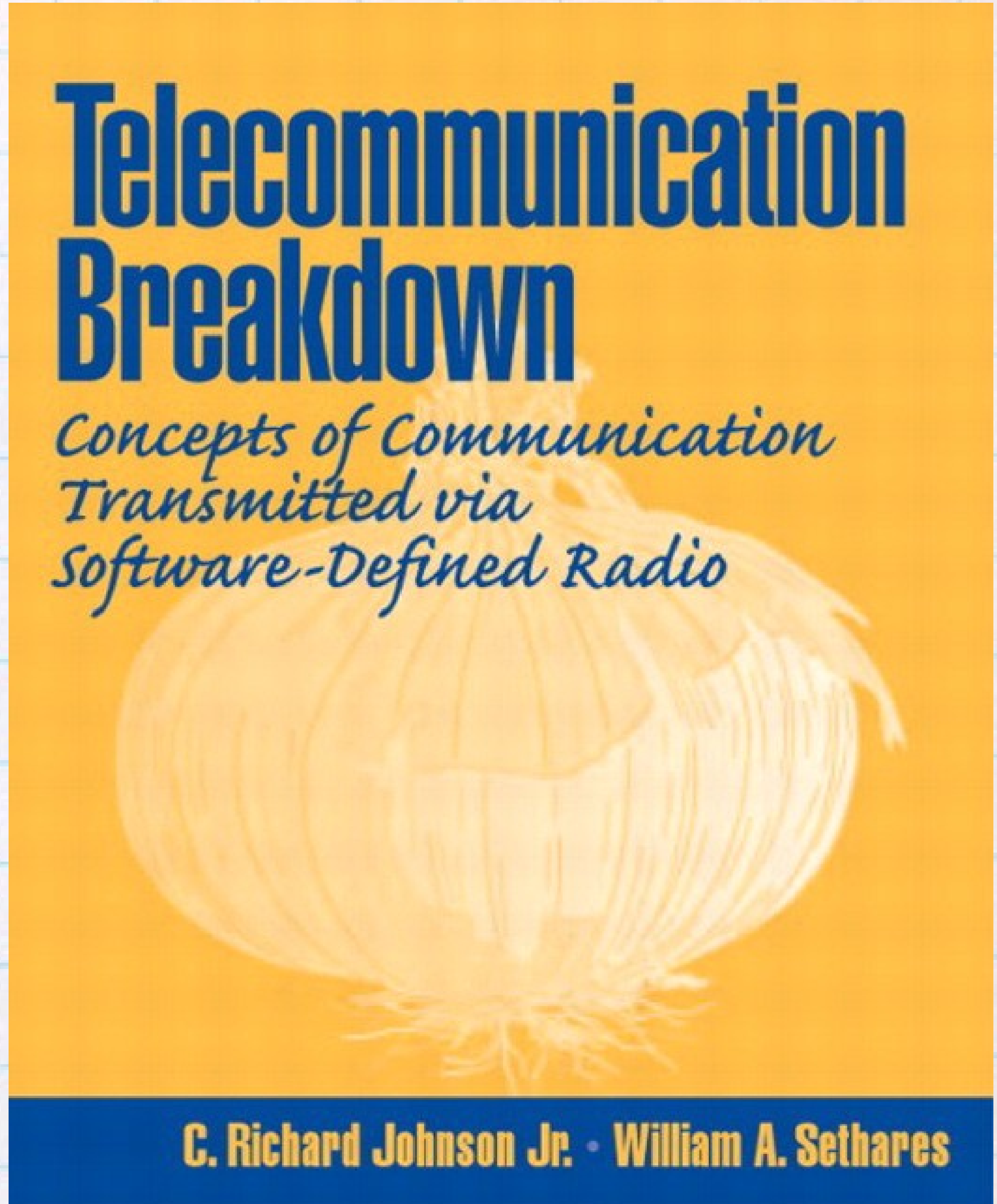
baudline



-5000
-2500
0
2500
5000
7500 Hz
2000
3000
4000
5000
ms


reuse, recycle

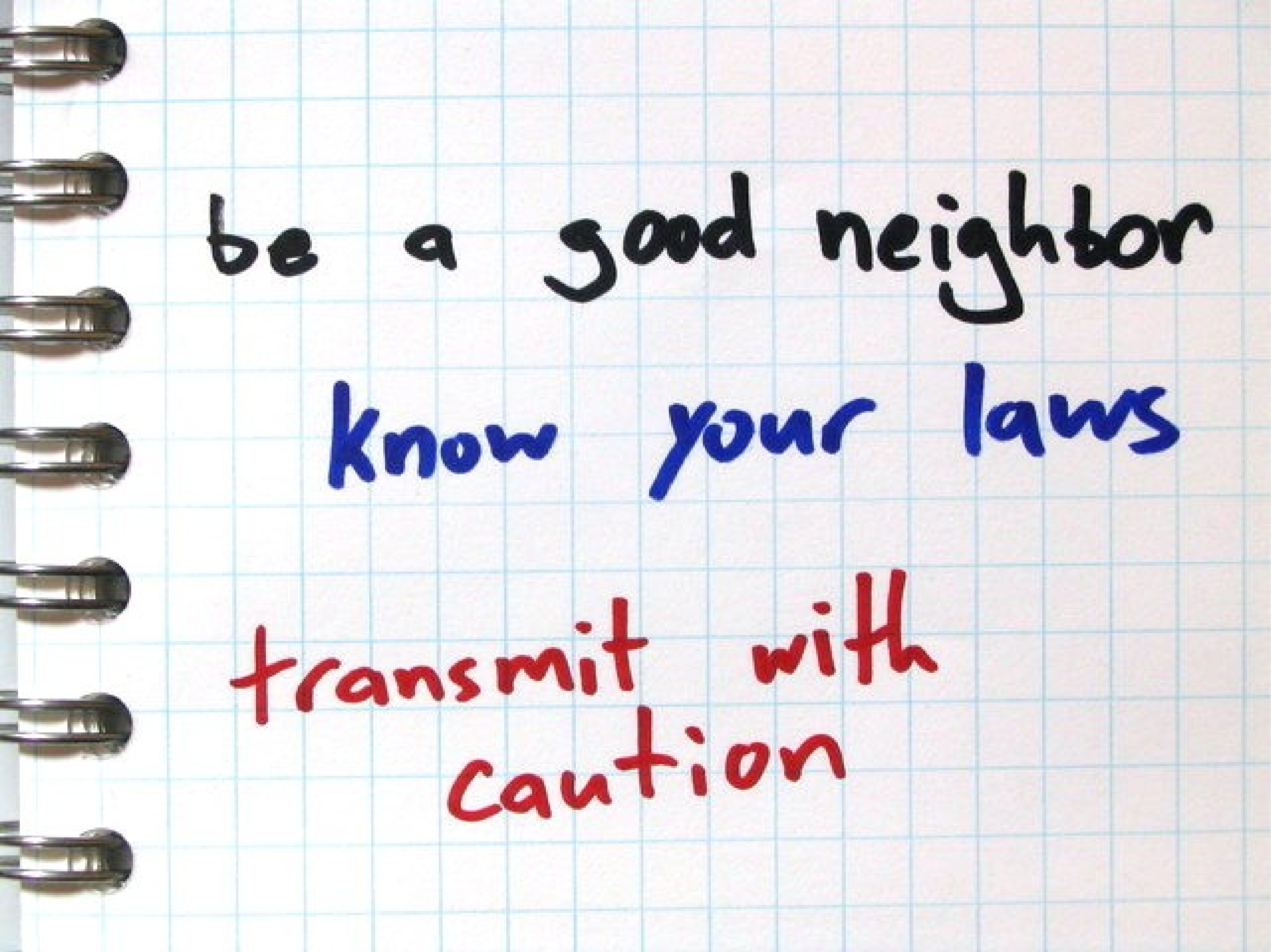
a good book


Telecommunication Breakdown
Concepts of Communication Transmitted via Software-Defined Radio
C. Richard Johnson Jr. • William A. Sethares

beyond radio communications

Van Eck

wires


be a good neighbor
know your laws
transmit with caution

http://ossmann.com/

bh-usa-08/

C. R. Johnson, Jr. and W. A. Sethares. Telecommunication Breakdown: Concepts of Communication Transmitted via Software-Defined Radio.
http://eceserv0.ece.wisc.edu/~sethares/telebreak.html

The GSM Software Project
http://wiki.thc.org/gsm

Max Moser and Phill Schrödel. 27Mhz based wireless security insecurities. http://www.remote-exploit.org/advisories.html

Dominic Spill and Andrea Bittau. BlueSniff: Eve meets Alice and Bluetooth.
http://www.usenix.org/event/woot07/tech/full_papers/spill/

Henryk Plötz. RFID Hacking.
http://events.ccc.de/congress/2006/Fahrplan/events/1576.en.html

olleB. Mobitex Network Security.
http://cansecwest.com/csw08/csw08-olleb.pdf
http://www.toolcrypt.org/

Daniel Halperin, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.
http://www.secure-medicine.org/icd-study/icd-study.pdf

GNU Radio: the gnu software radio.
http://gnuradio.org/trac

The Universal Software Radio Peripheral (USRP).
http://www.ettus.com/

High Performance Software Defined Radio.

http://hpsdr.org/

baudline signal analyzer.

http://www.baudline.com/

MATLAB.

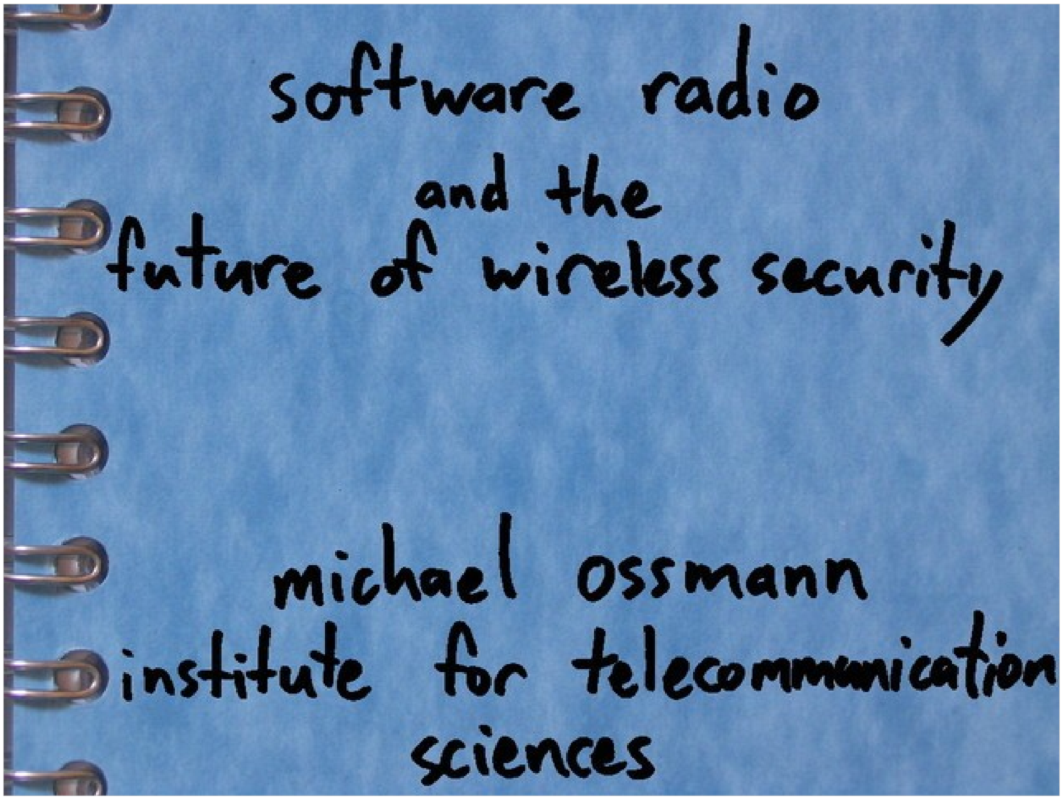
http://www.mathworks.com/

GNU Octave.

http://www.gnu.org/software/octave/

OP25. A software-defined analyzer for APCO P25 signals.

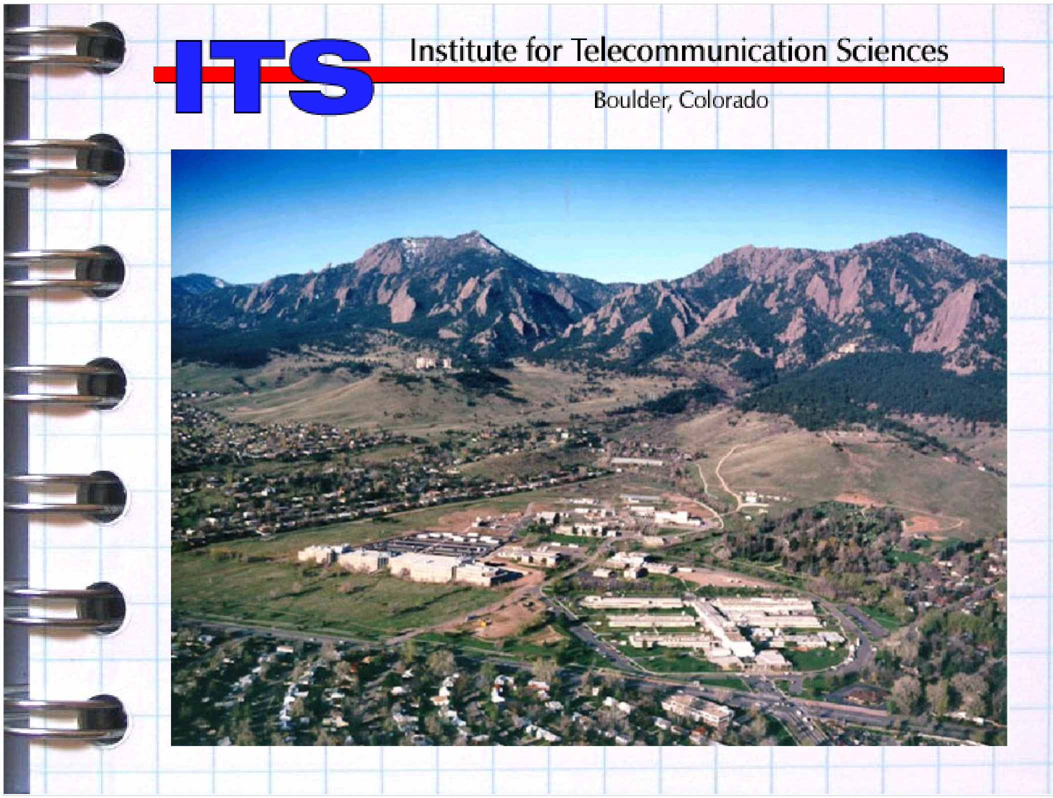
http://sedition.org.au/op25



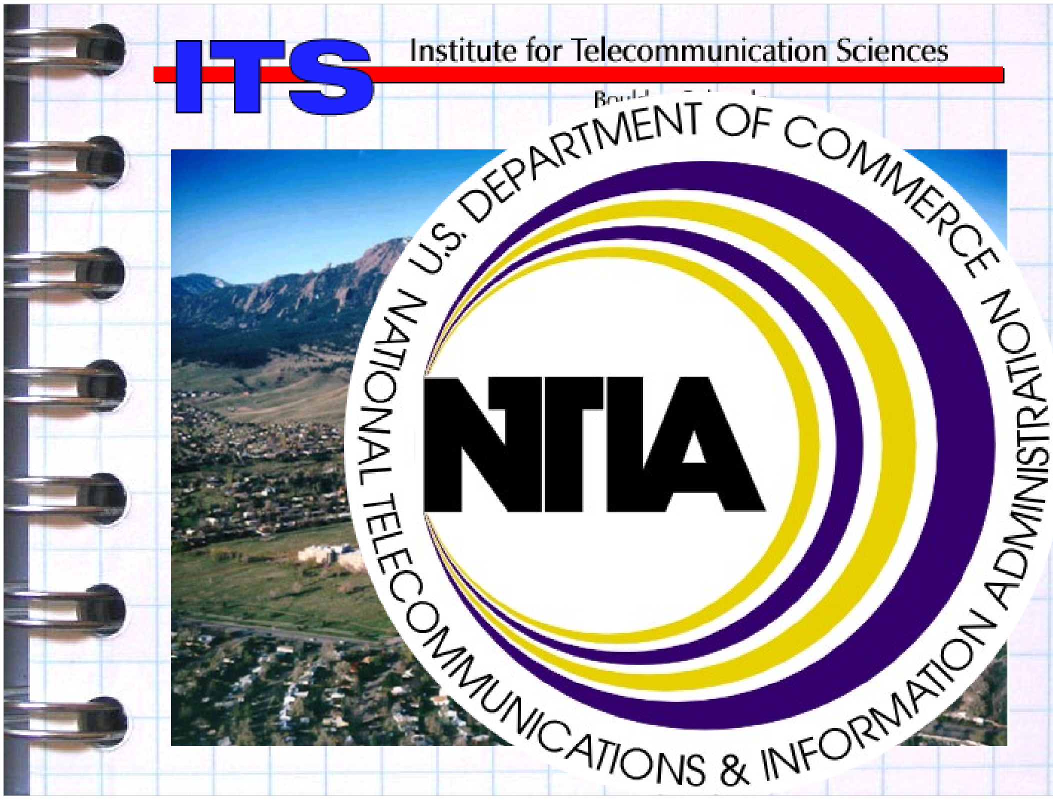
Software Radio and the Future of Wireless Security

Michael Ossmann
Institute for Telecommunication Sciences

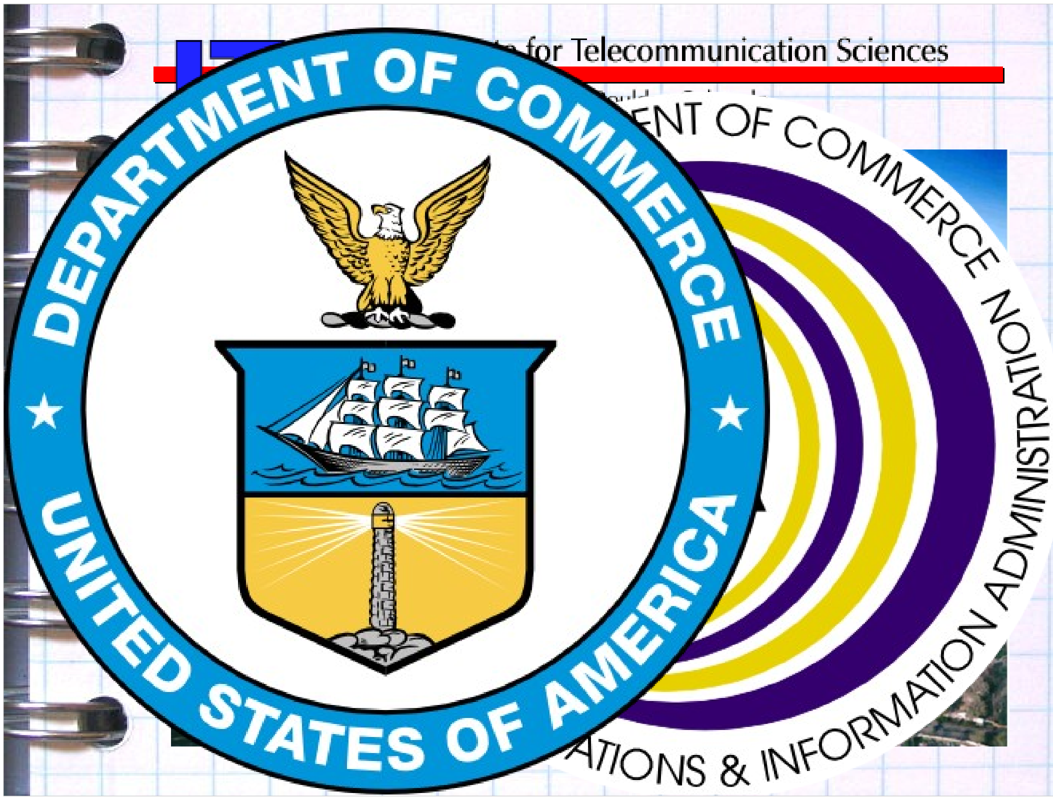
This presentation is an outgrowth of work done under contract to the Institute for Telecommunication Sciences and does not represent the views or policies of the United States federal government.



My name is Michael Ossmann. I work for the Institute for Telecommunication Sciences at the Boulder Labs in Colorado.

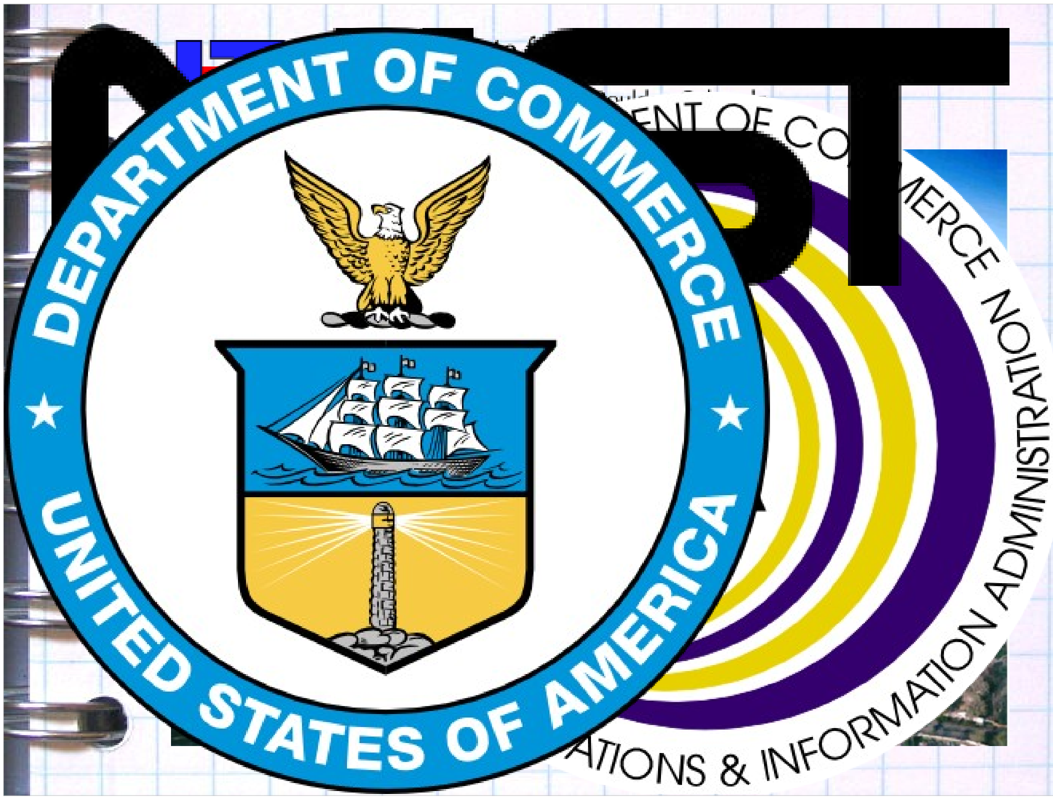


ITS is part of the National Telecommunications and Information Administration.



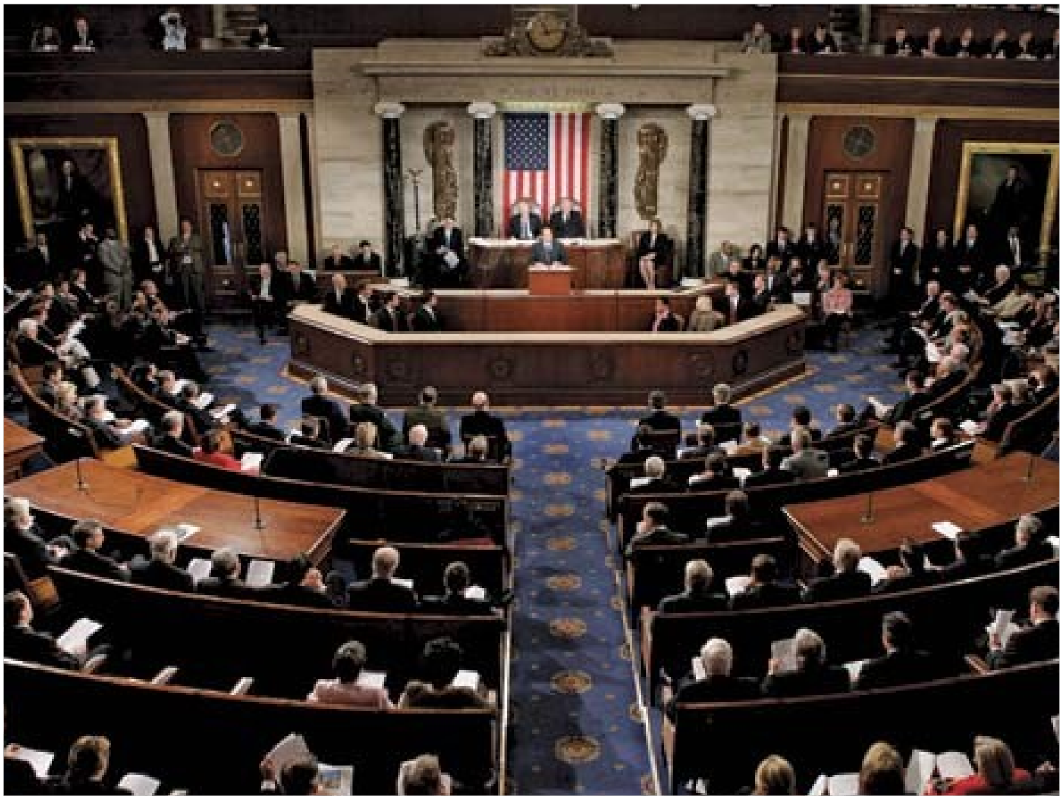
The NTIA is part of the United States Department of Commerce.

I work primarily on public safety wireless communication security, and my work is funded by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.



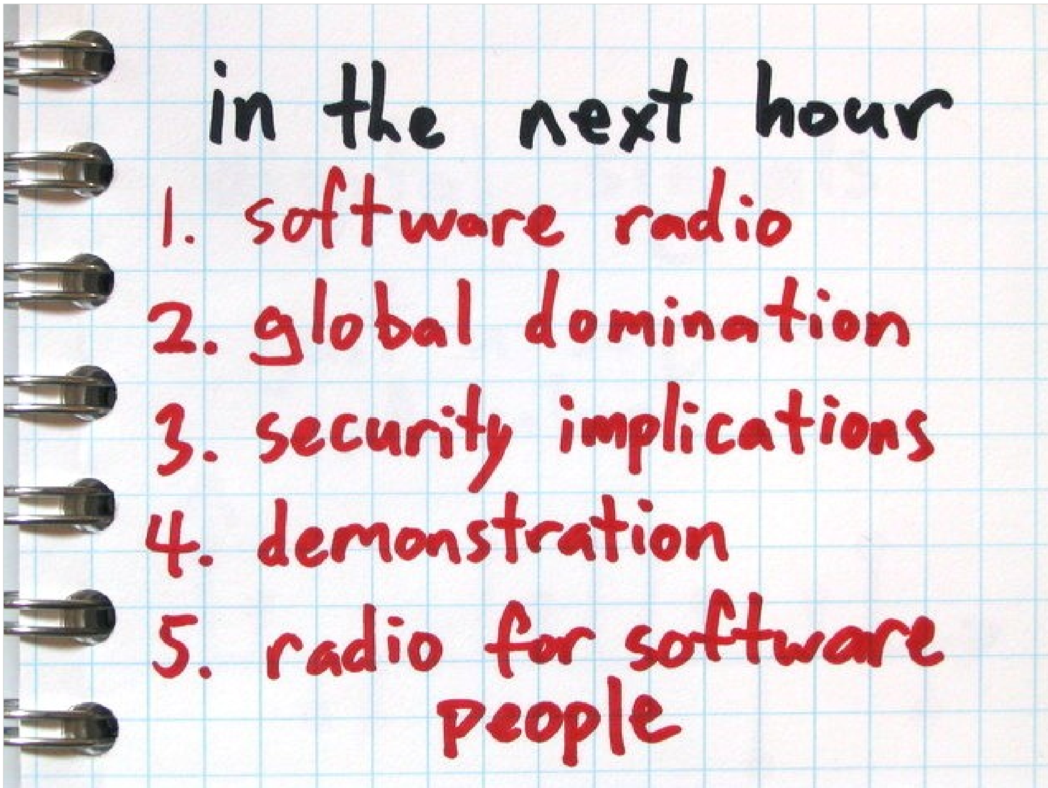
NIST is also part of the Department of Commerce.

NIST's funding for my work comes from the Department of Homeland Security's Office for Interoperability and Compatibility.



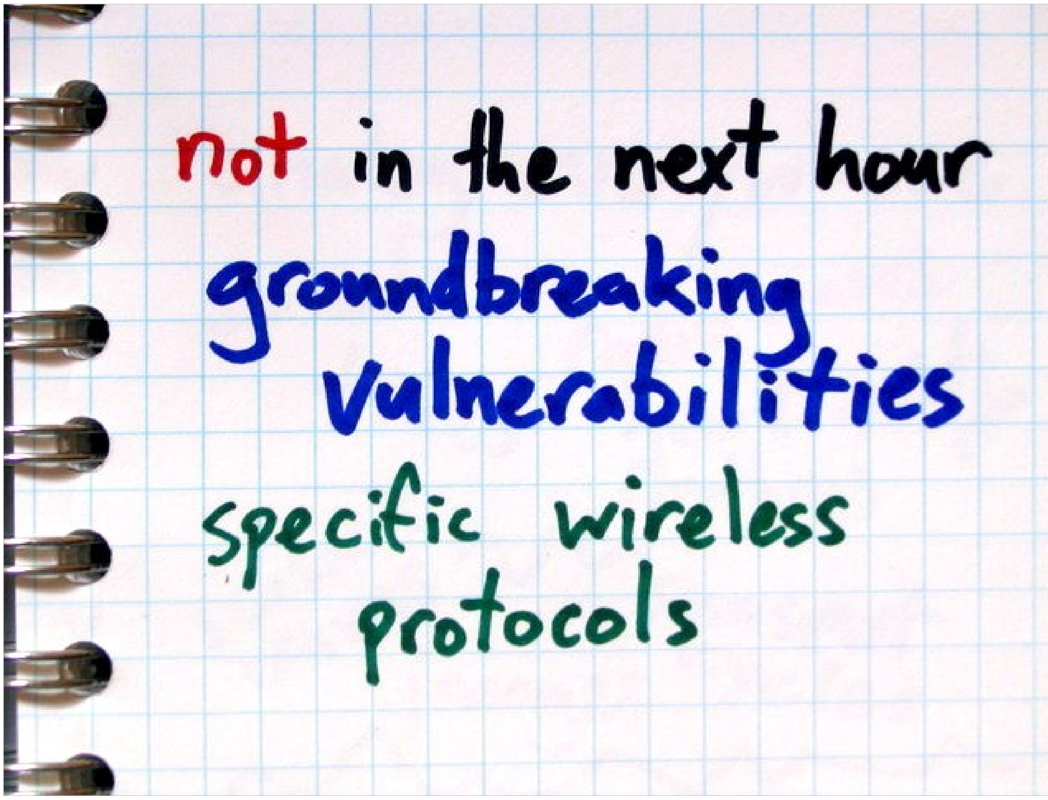
DHS gets its money from these guys


Security
Smart Business.



in the next hour

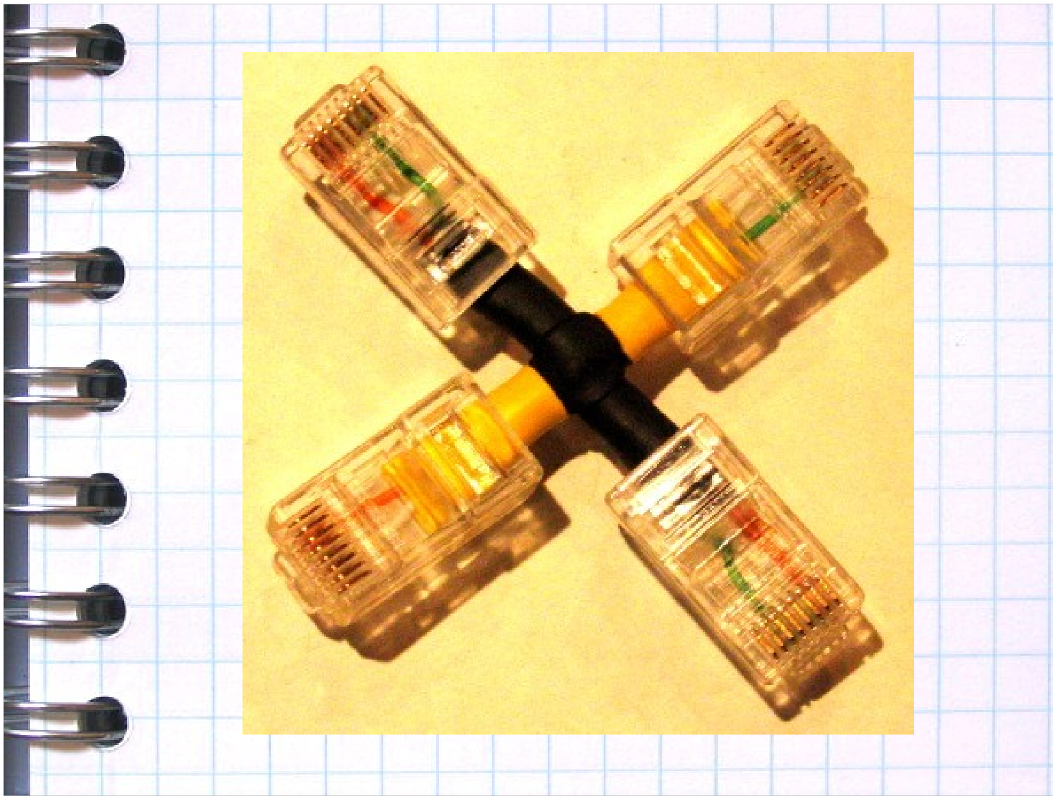
what is software radio?
why is software radio taking over the world?
what does this mean for the future of wireless security research?
demos
how can I get started with software radio tools today? (radio for software people)

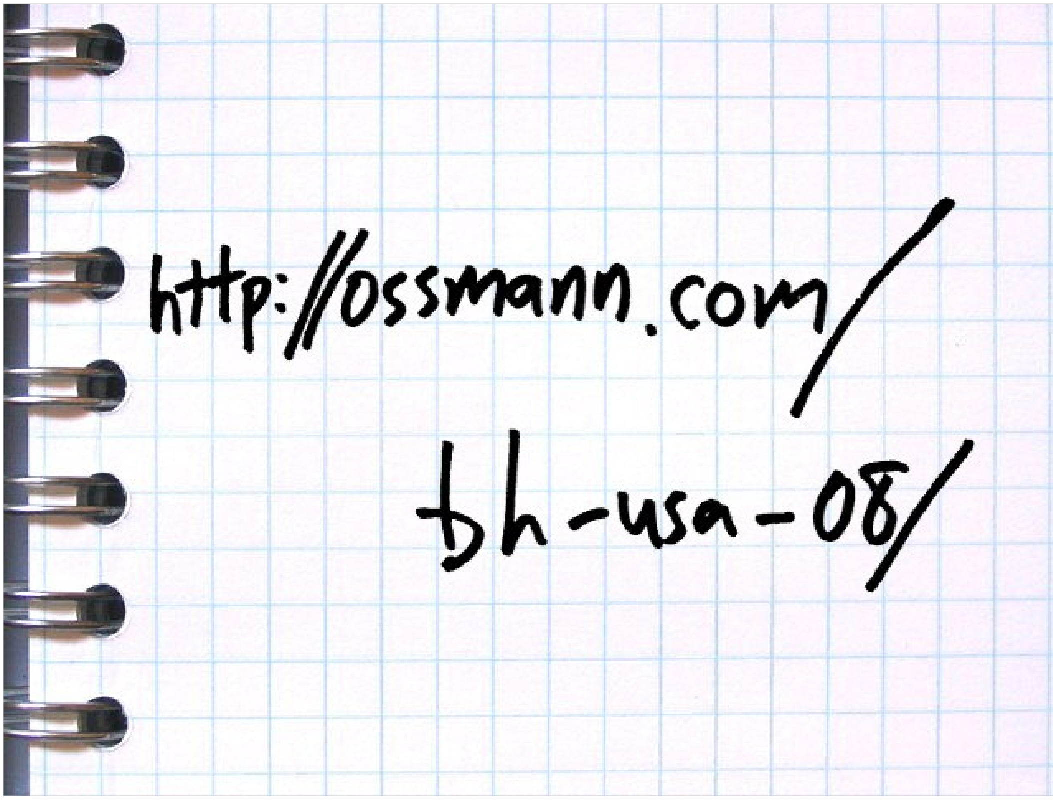


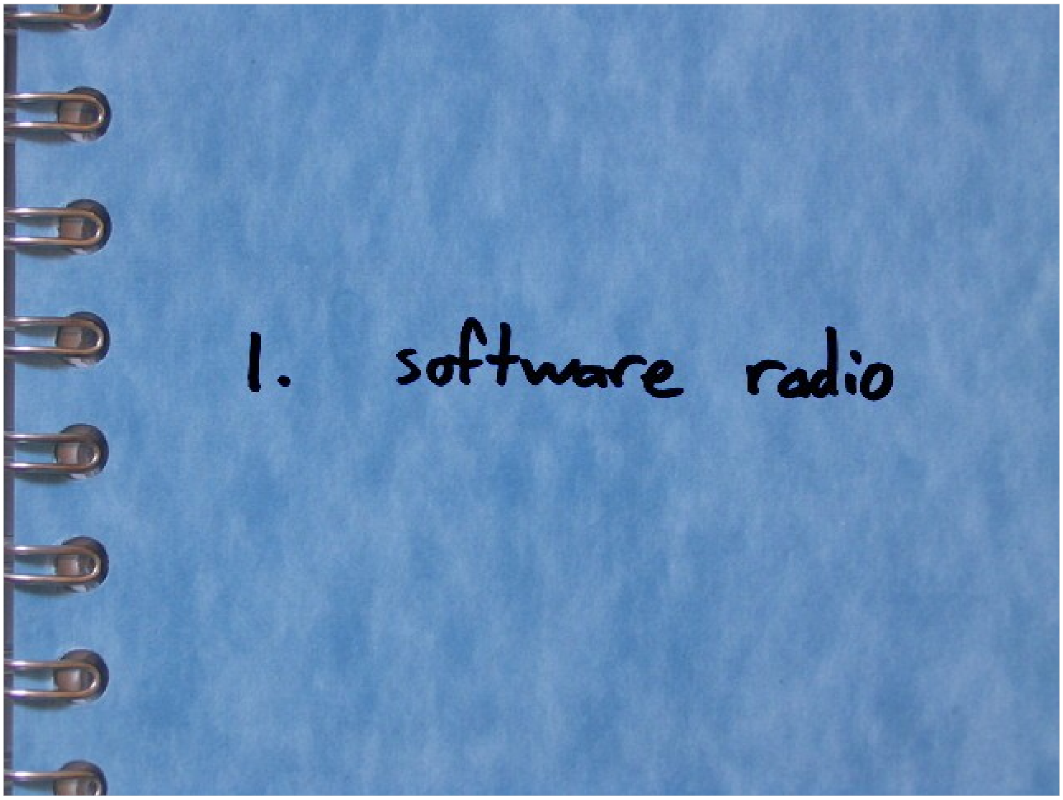
not in the next hour

groundbreaking vulnerabilities
specific wireless protocols

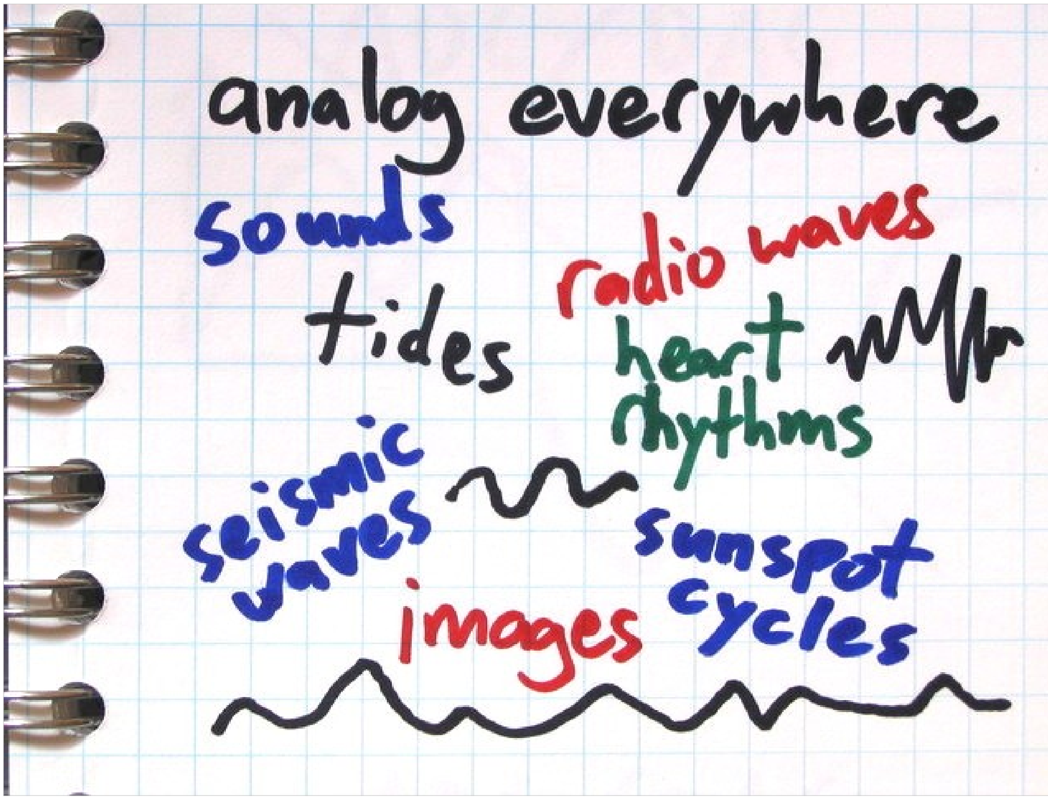

Mystery
Signal
Challenge!




http://ossmann.com/
bh-usa-08/

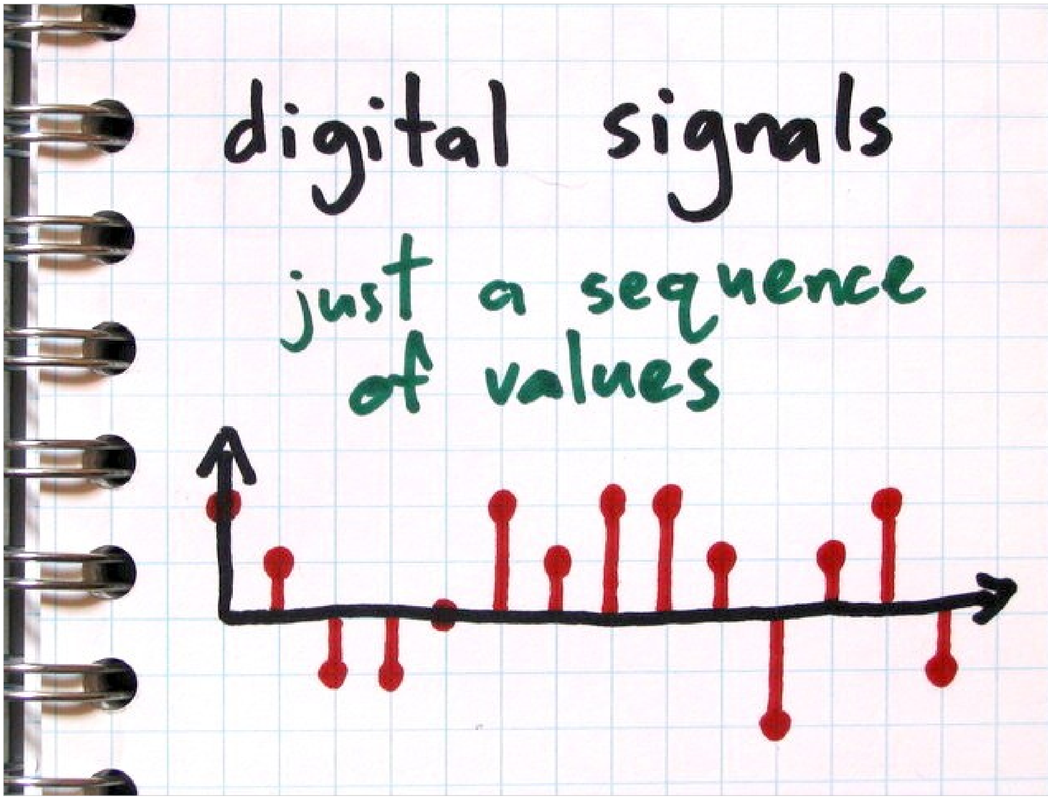


1. what is software radio?



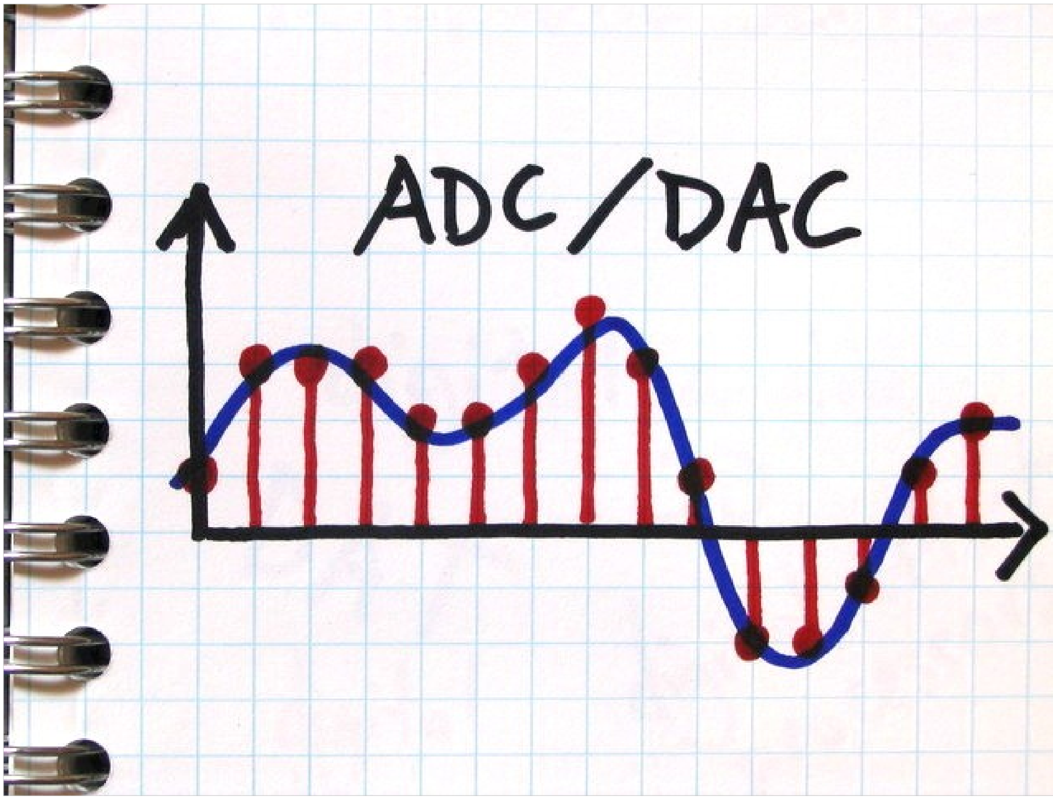
analog signals surround us

sounds
images
radio waves
tides
heart rhythms
seismic waves
anything that changes over time



digital signals

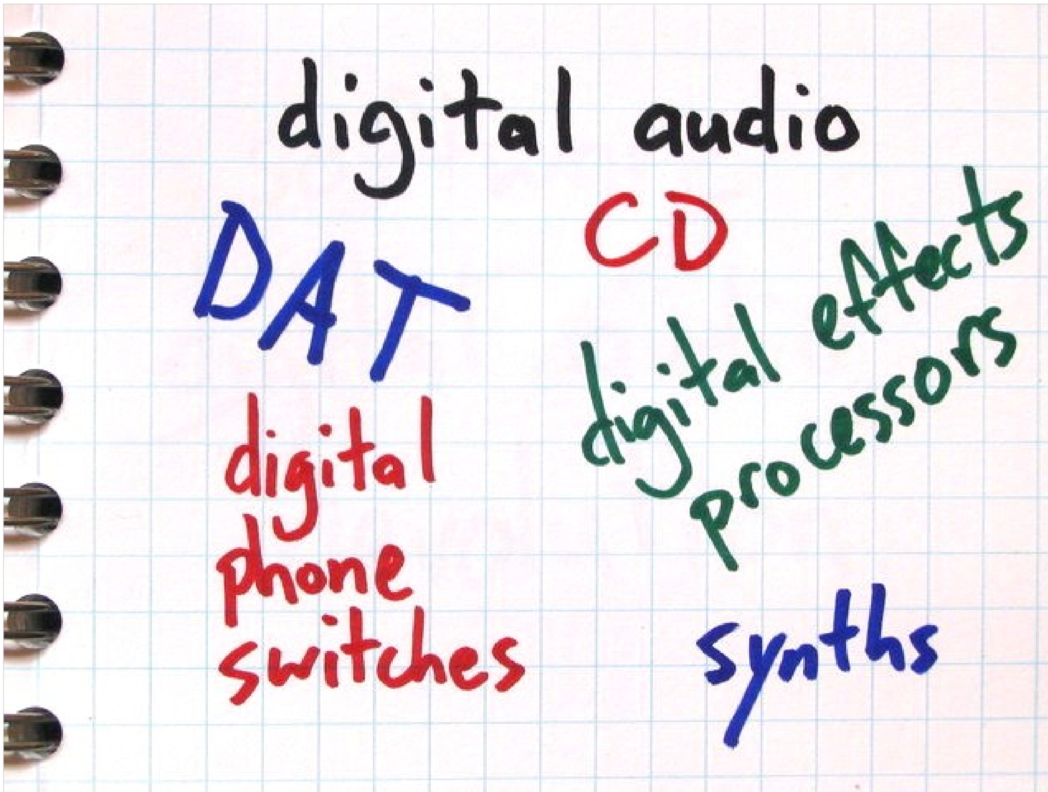
- a digital signal is simply a sequence of values
- analog signals can be sampled to produce digital signals


ADC / DAC

the digital audio revolution

once upon a time, all sound was analog:

- vinyl records
- analog tape
- analog synthesizers
- analog effects
- Plain Old Telephone Service



the digital audio revolution

the revolution began slowly:
- Digital Audio Tape (DAT)
- Compact Discs (CDs)
- digital synthesizers
- digital effects
- digital telephone switches

individual digital components replaced traditional analog components

professional equipment used by professionals

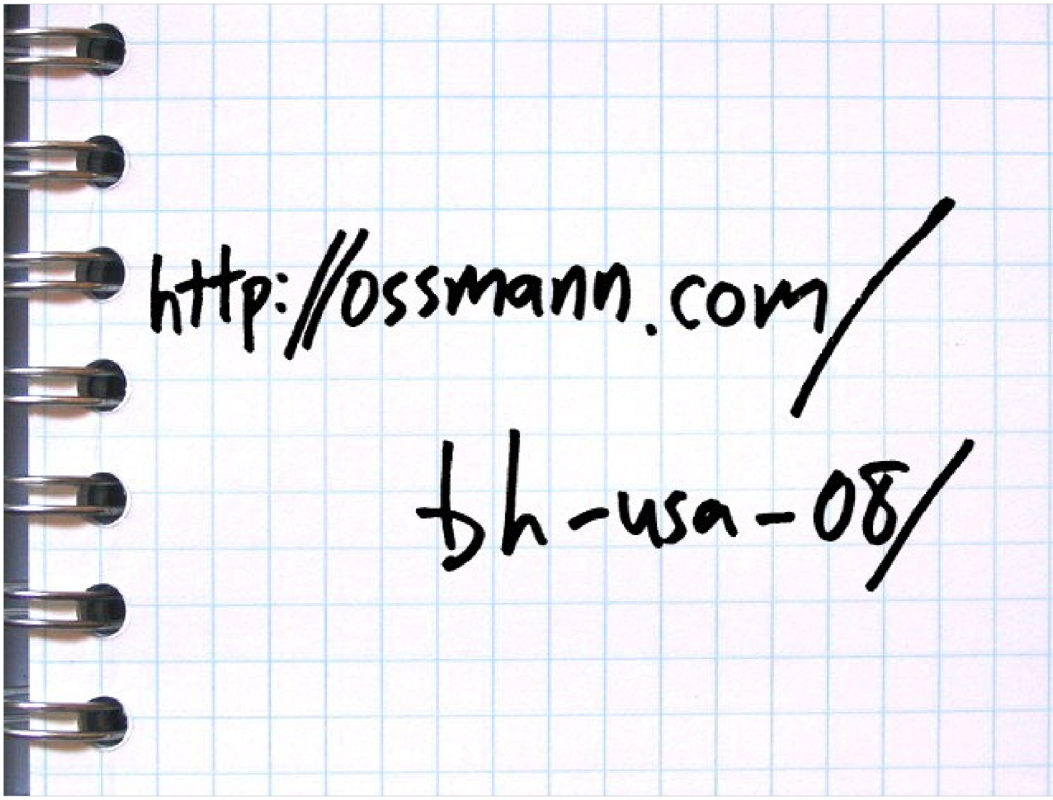
the digital audio revolution

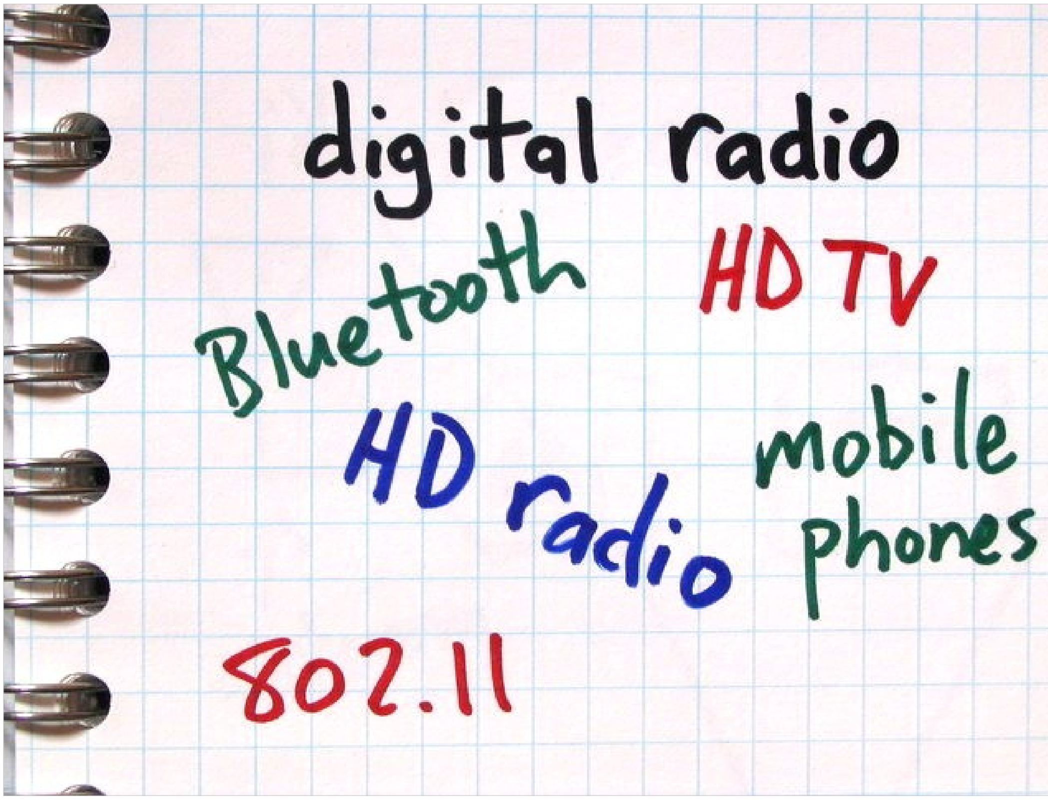
then the explosion:
- hard disc recording
- home recording studios
- MP3
- peer to peer (Napster, Skype, etc.)
- analog modeling digital synthesizers

personal computers delivered professional audio tools to the masses
today:
- many of today's hits are recorded in home studios
- old school record labels struggle to compete with new distribution channels
- VoIP services challenge incumbent telephone companies

why the explosion?

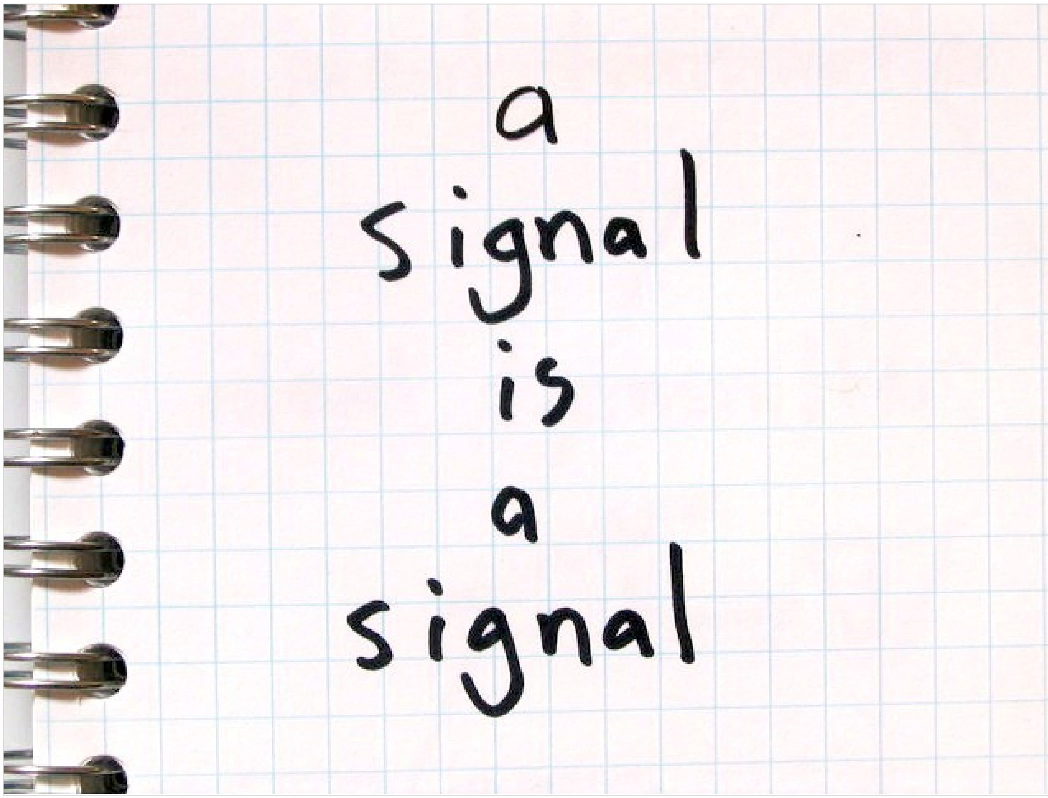
- digital audio circuitry had existed for many years
- personal computers enabled wide distribution of software-based digital audio processing
- digital audio brought incremental change, but **software audio** was the true revolution


http://ossmann.com/
bh-usa-08/



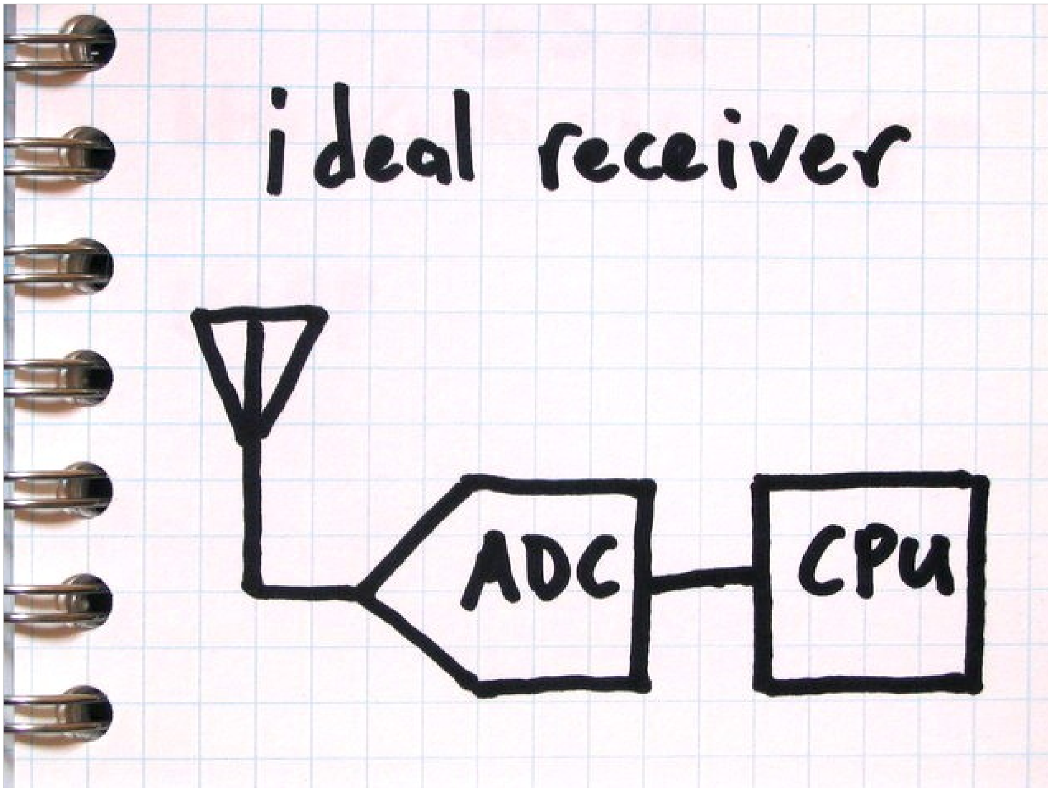
digital radio

nearly every recent radio technology is digital:
- 802.11
- HD radio and TV
- mobile phones
- Bluetooth



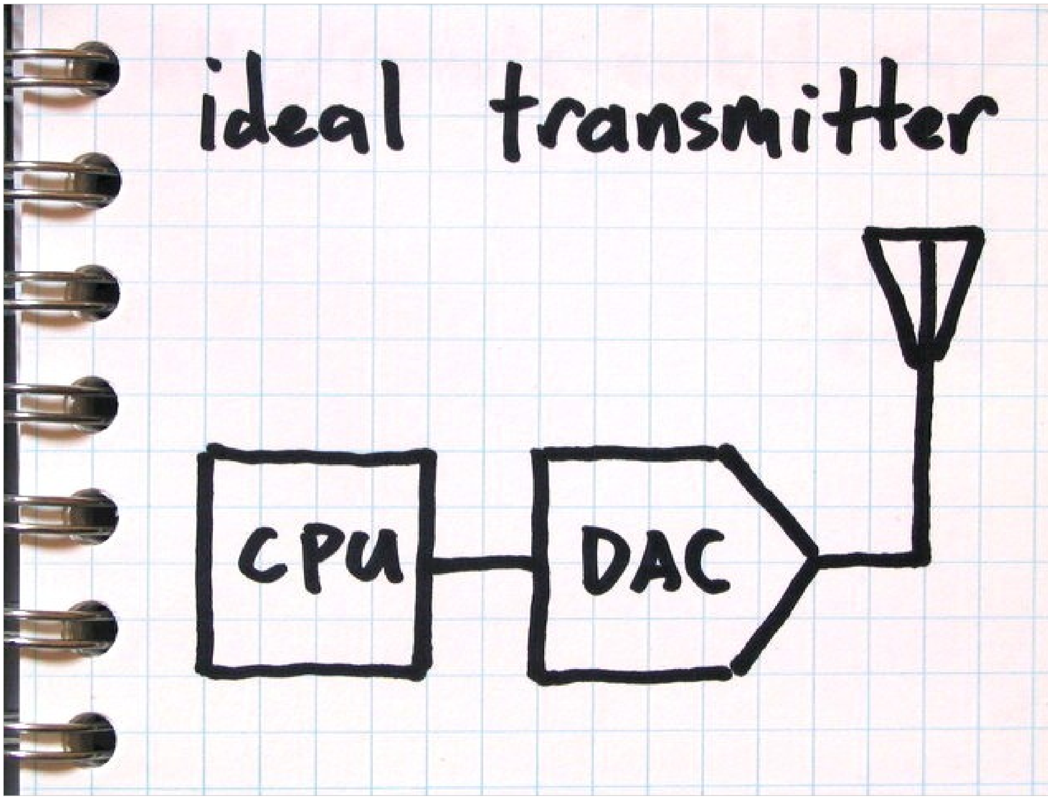
software radio

- a signal is a signal (if it can be done with audio, it can be done with radio)
- personal computers are now fast enough for many radio processing functions



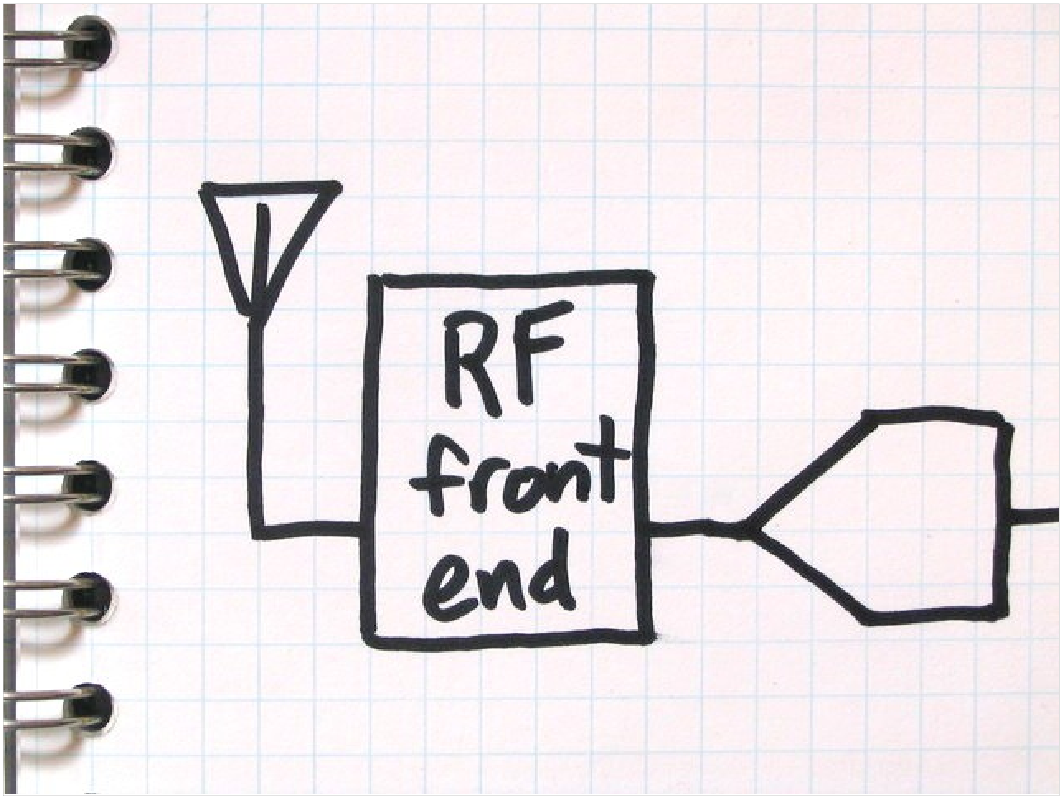
ideal software radio receiver

antenna -> ADC -> CPU



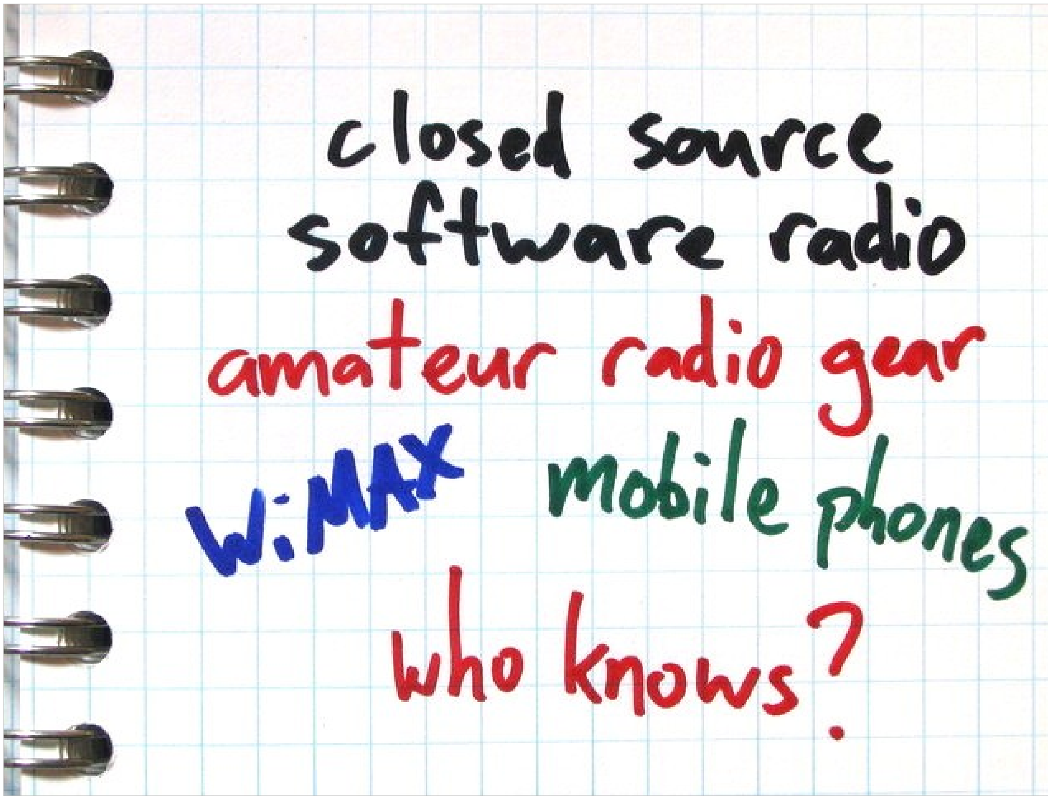
ideal software radio transmitter

CPU -> DAC -> antenna



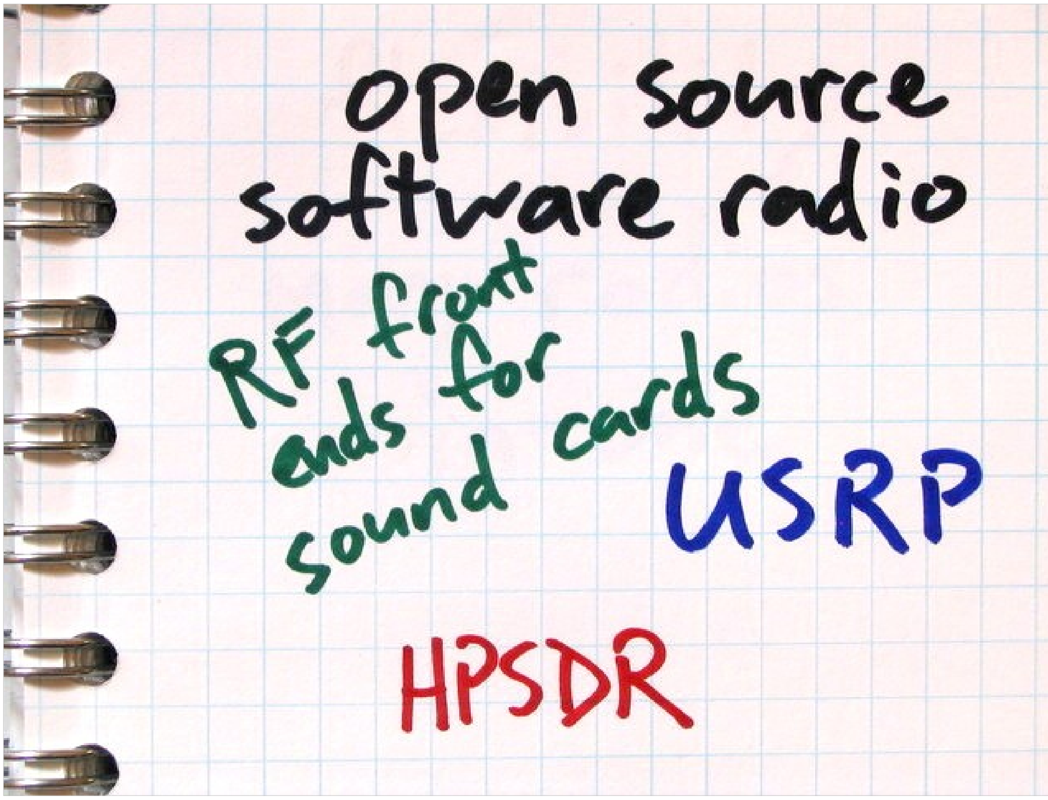
practical software radio

RF front end (analog circuit) is typically required
- frequency conversion
- amplification
- filtering
- bias



software radio products

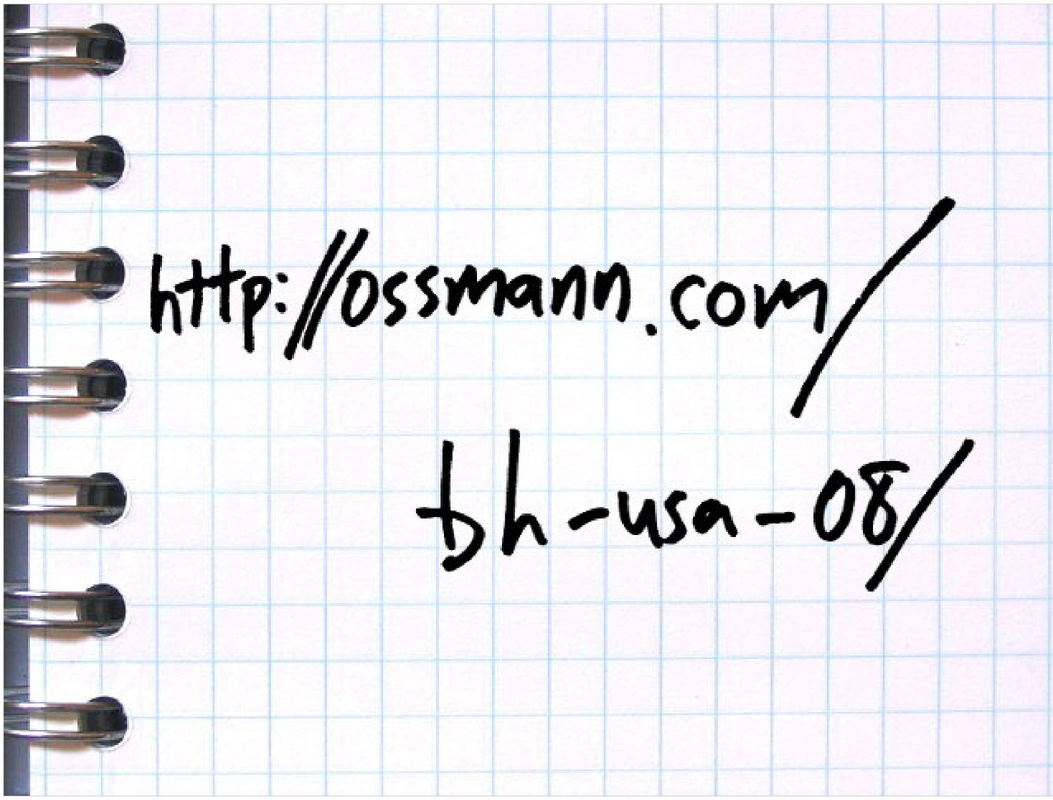
- more and more closed source commercial devices
  - use software (or firmware) radio techniques
    - amateur radio equipment
    - WiMAX equipment
    - mobile phone base stations
    - a few mobile phones
- several commercial software radio products for PCs
  - most are RF front ends for sound cards


open source
software radio
RF front
ends for
sound cards
USRP
HPSDR

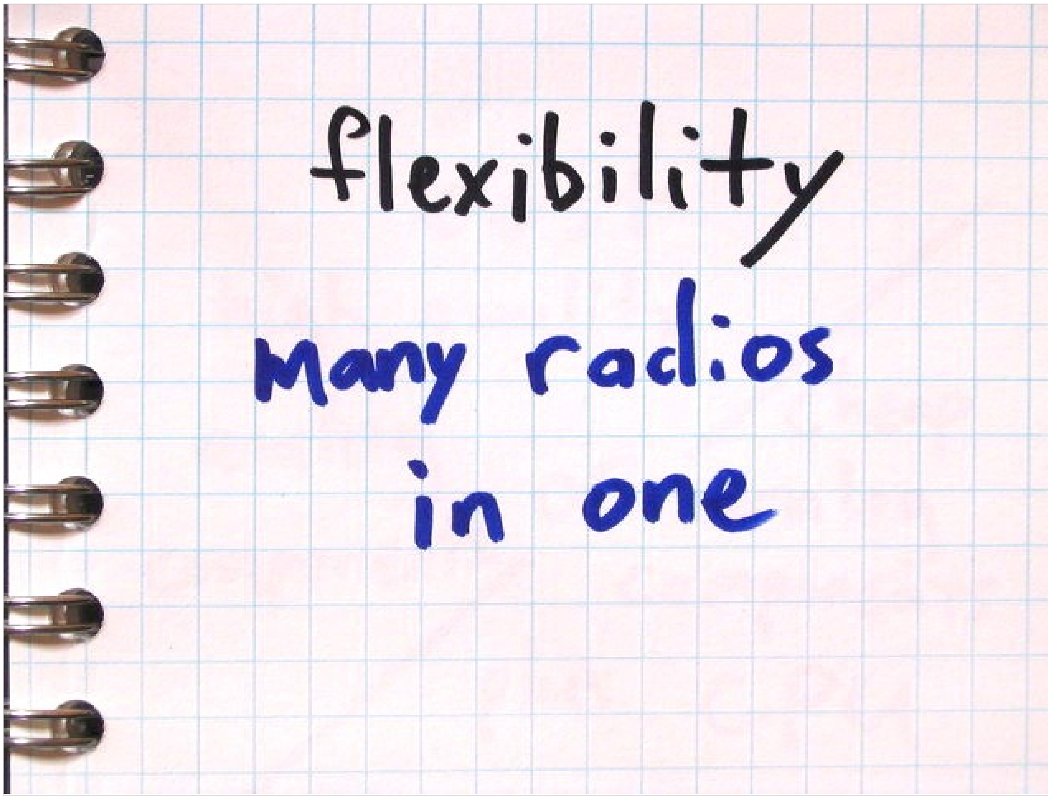
The Universal Software Radio Peripheral (USRP)

http://www.ettus.com/

open source design
can receive and transmit
multiple RF front end daughterboards
ADC/DACs
FPGA
USB
GNU Radio interface


http://ossmann.com/
bh-usa-08/

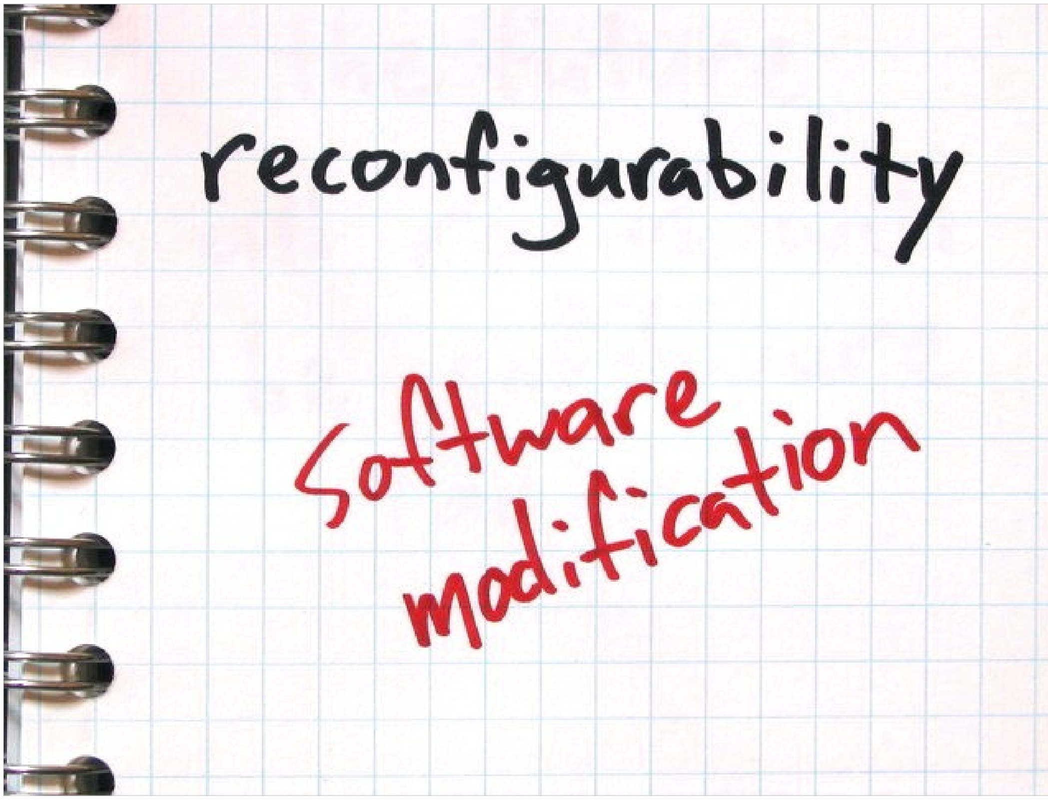
2. why is software radio taking over the world?



advantage: flexibility

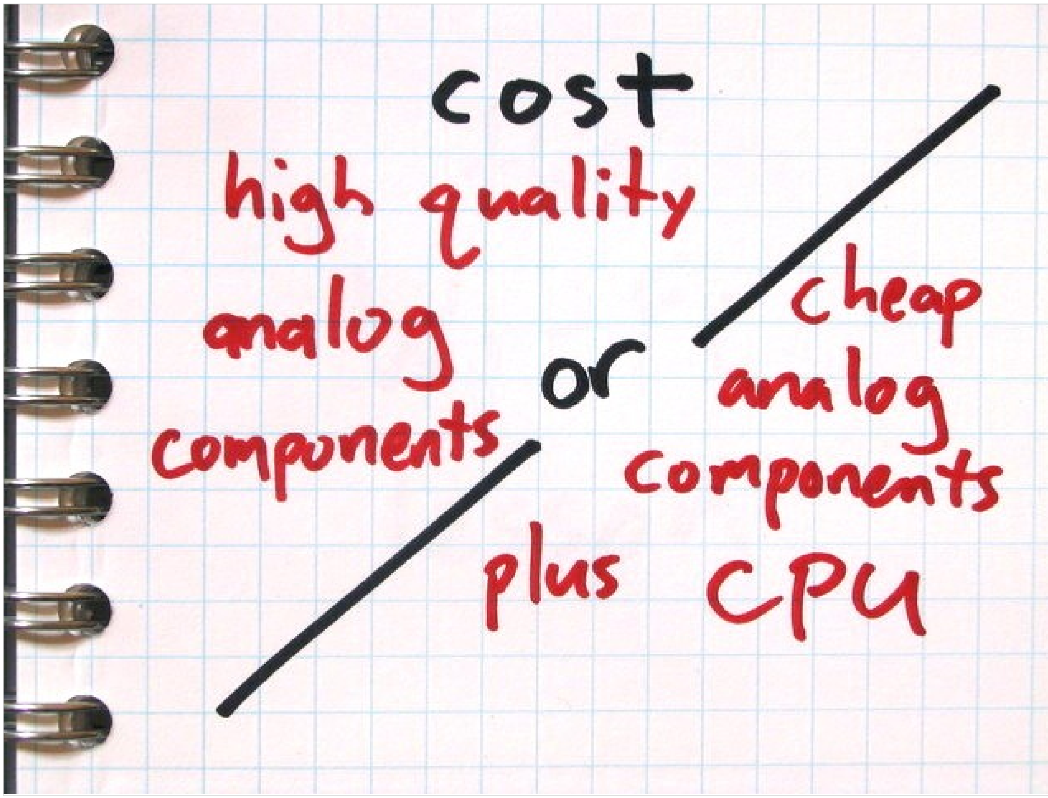
software radios can have many operating modes
without many circuits

software radios can perform like multiple radios
simultaneously



advantage: reconfigurability

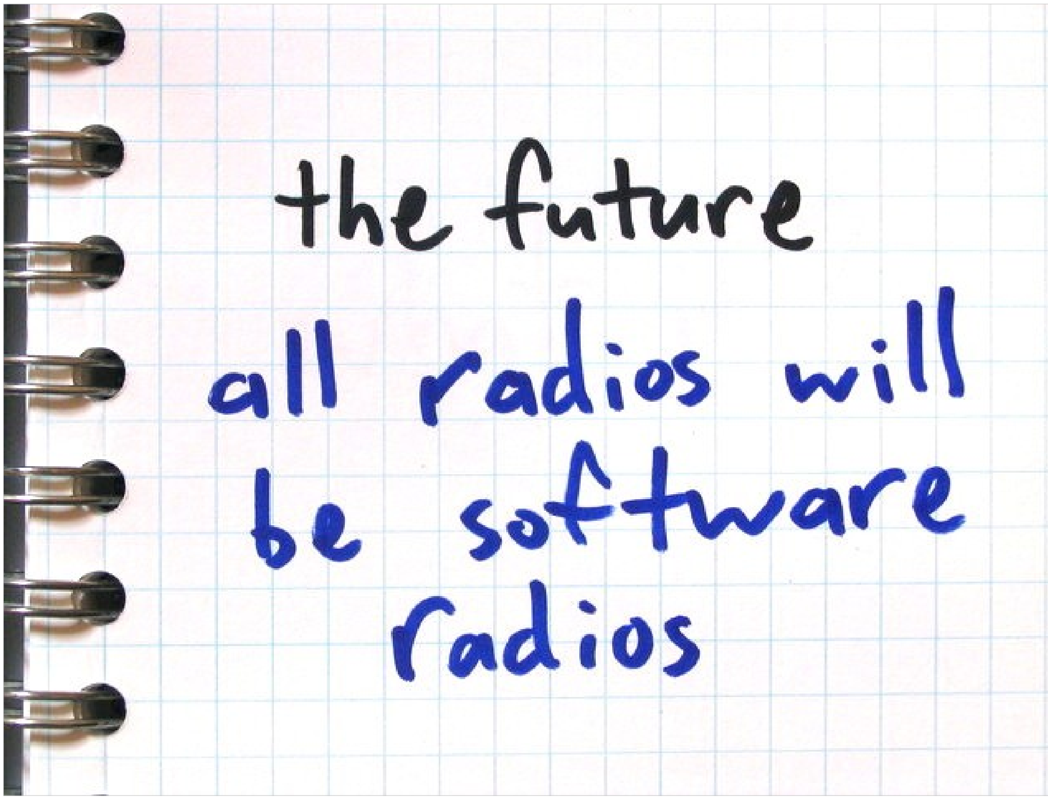
- software radios can implement new software at any time
  - new protocols
  - adaptive filtering
  - new frequencies
  - bug fixes
  - hacks!
- with open source, new radio functions can easily be shared online



advantage: cost

two ways to build a sophisticated radio device:

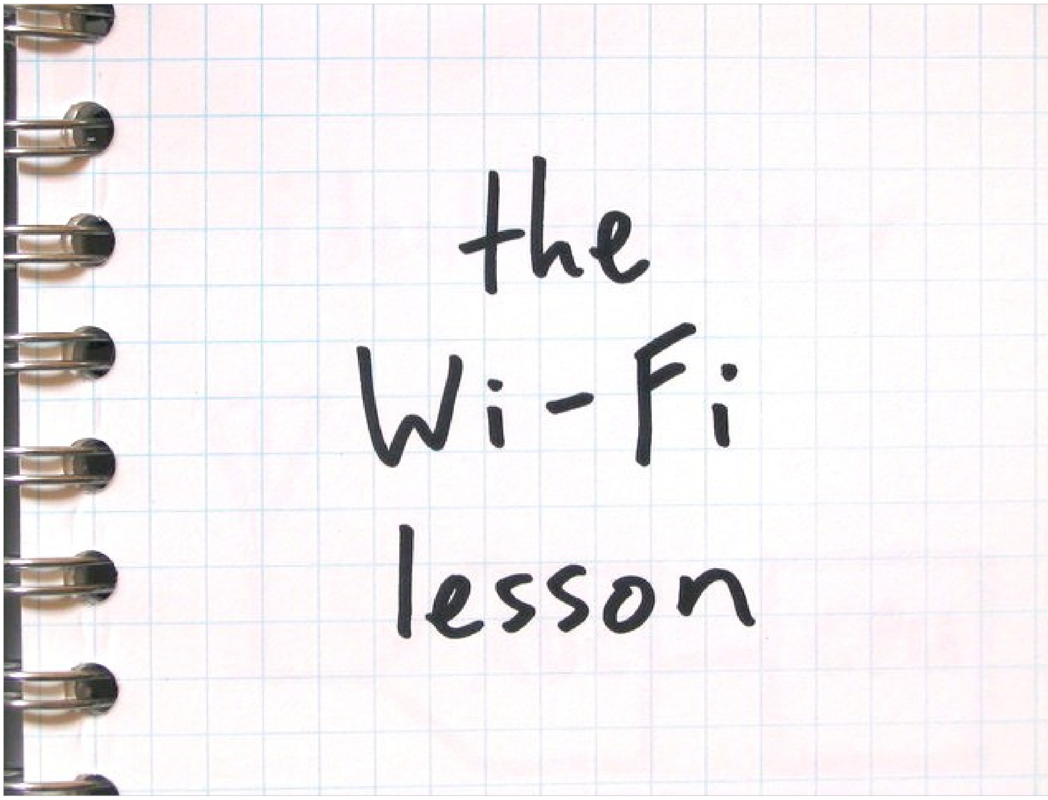
- lots of expensive analog components (and often some digital stuff too)
- a few cheap analog components plus a computer
  - consider Moore's Law
  - software can make up for deficiencies in the analog circuitry



the future

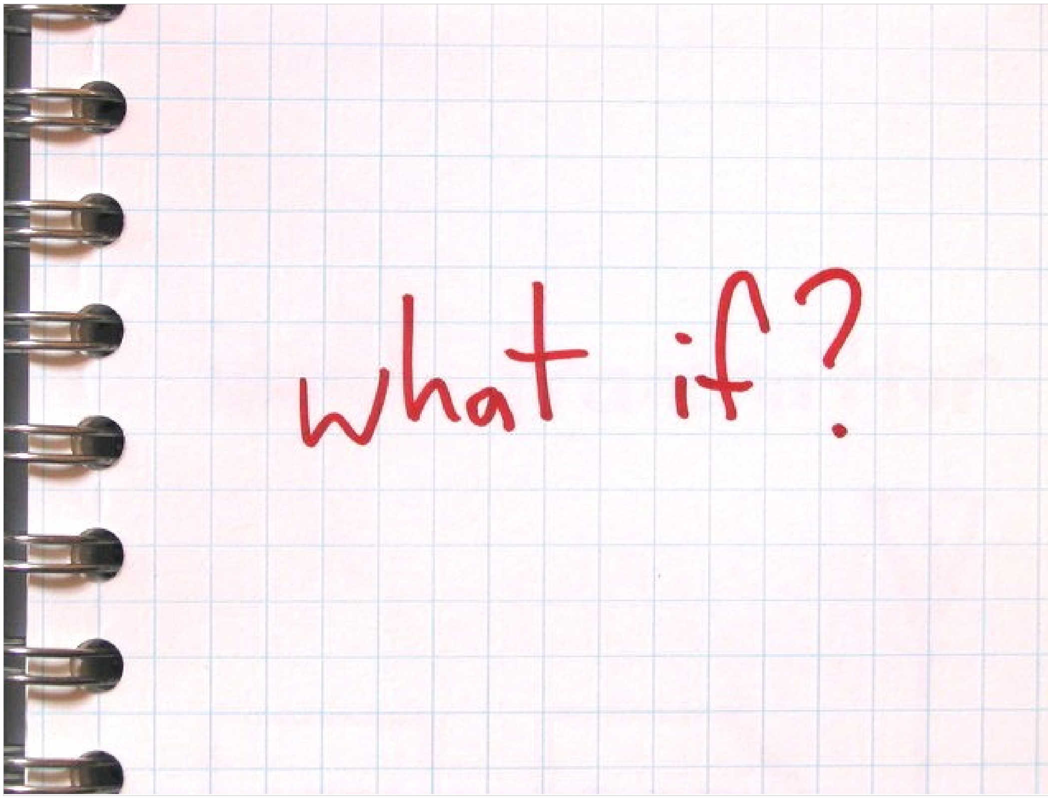
consider the commercial advantages of software radio
consider the current emergence of open source mobile phones and hand-held platforms (OpenMoko, Android, etc.)
consider that mobile phones using (closed source) software radio technology are starting to arrive
we will all have hackable software radio platforms in our pockets
all (okay, most) radios will be software radios
new wireless protocols will include software reference implementations during development
all wireless security tools will be software radios

3. what does this mean for wireless security?

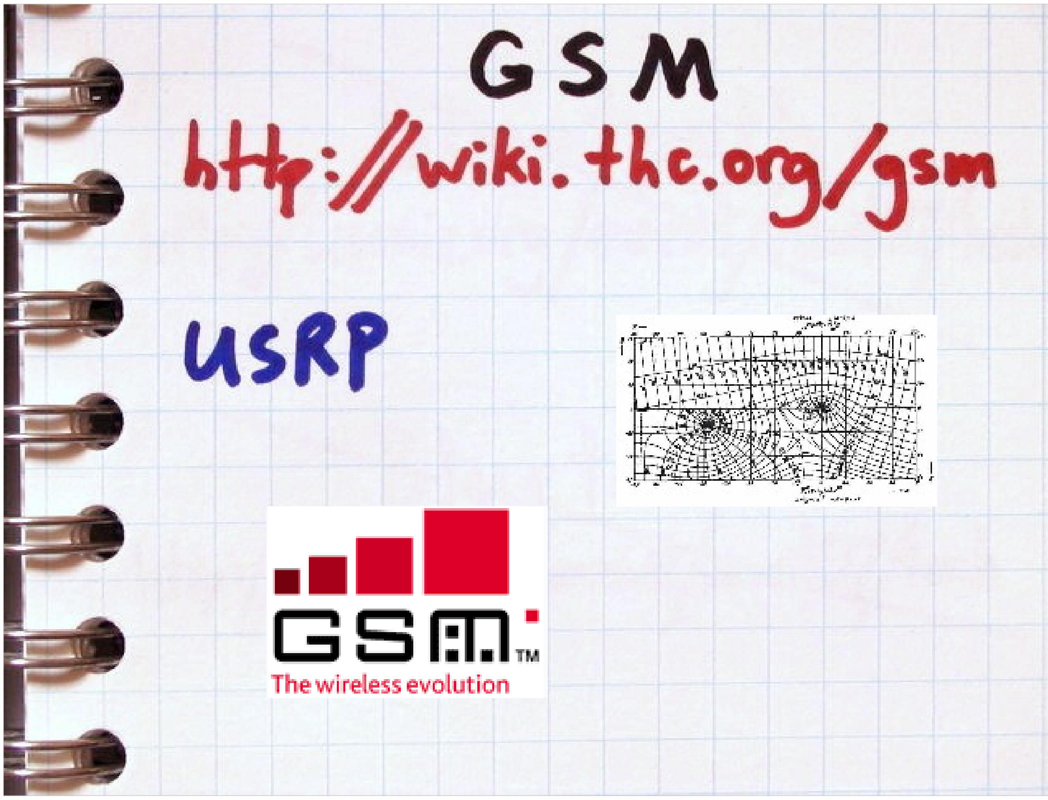


the Wi-Fi lesson

802.11b shipped with severe vulnerabilities
vulnerabilities were ignored until practically
demonstrated
practical attacks were made easy by cheap,
ubiquitous, hackable hardware:
monitor mode
raw frame injection

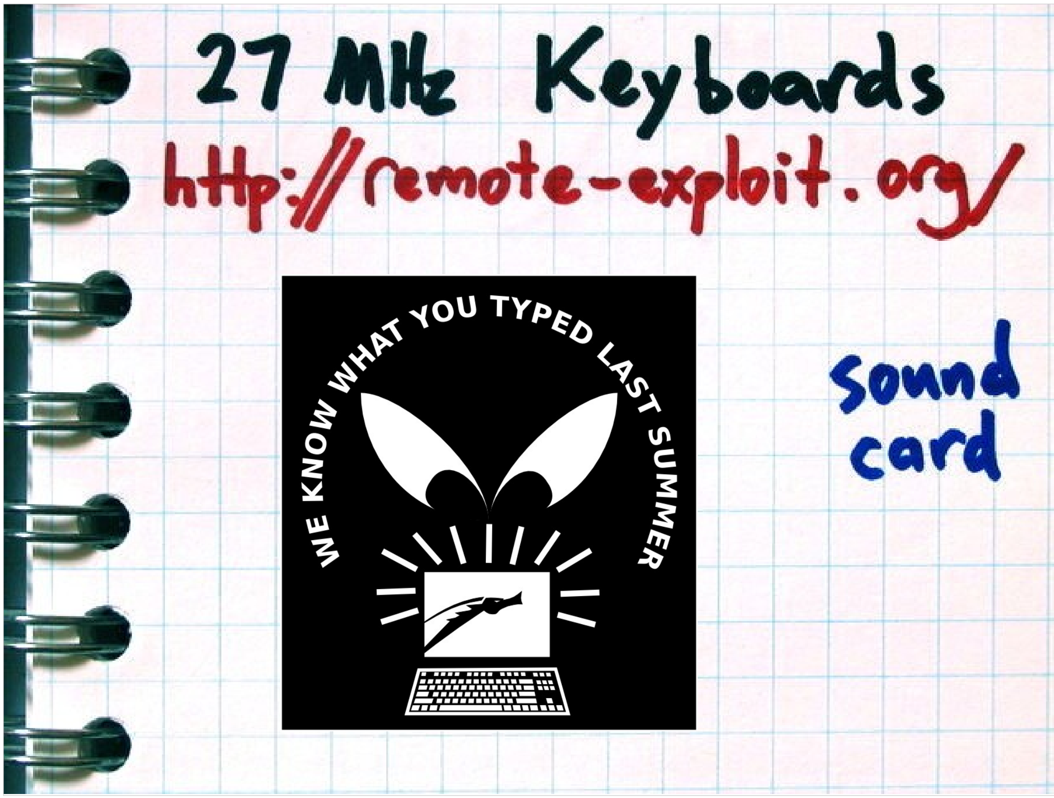


what if every new wireless technology arrived with inexpensive hardware capable of monitor mode and raw frame injection?



GSM
http://wiki.thc.org/gsm

USRP/GNU Radio
decoded GSM signals
related project: A5/1 decryption



27 MHz keyboards

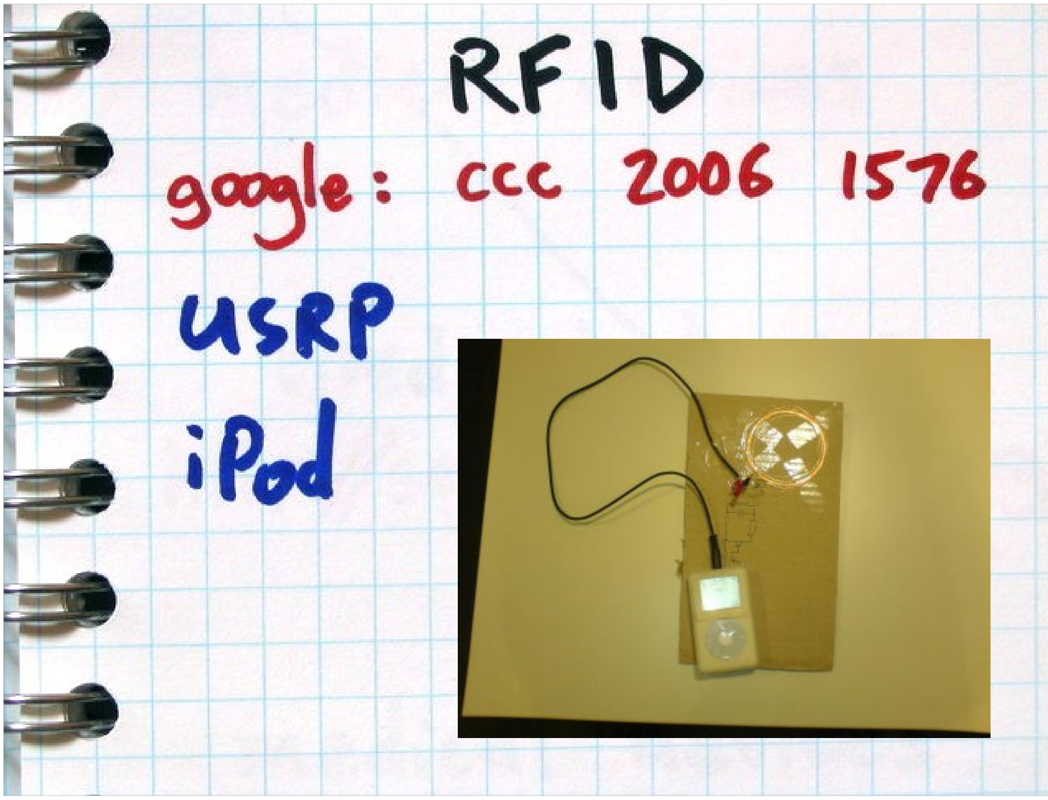
http://www.remote-exploit.org/advisories.html

sound card with RF front end
decrypted keystrokes

Bluetooth

http://www.usenix.org/event/woot07/tech/full_papers/spill/

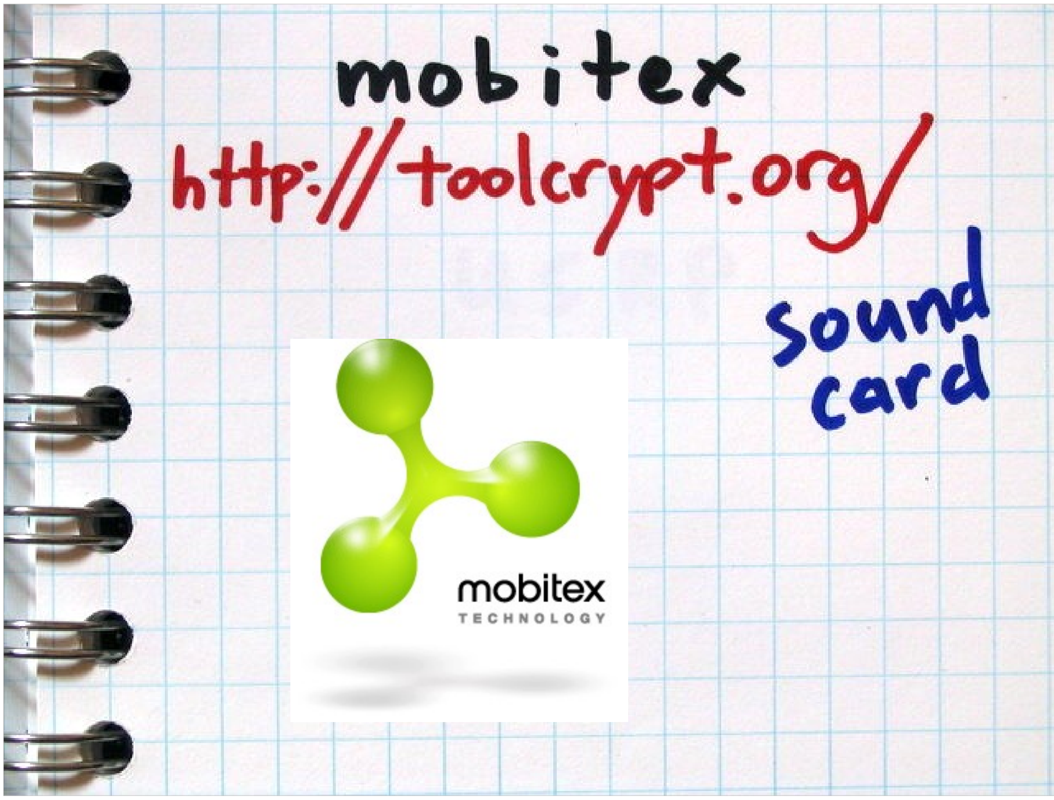
USRP/GNU Radio
single channel sniffing and decoding



RFID

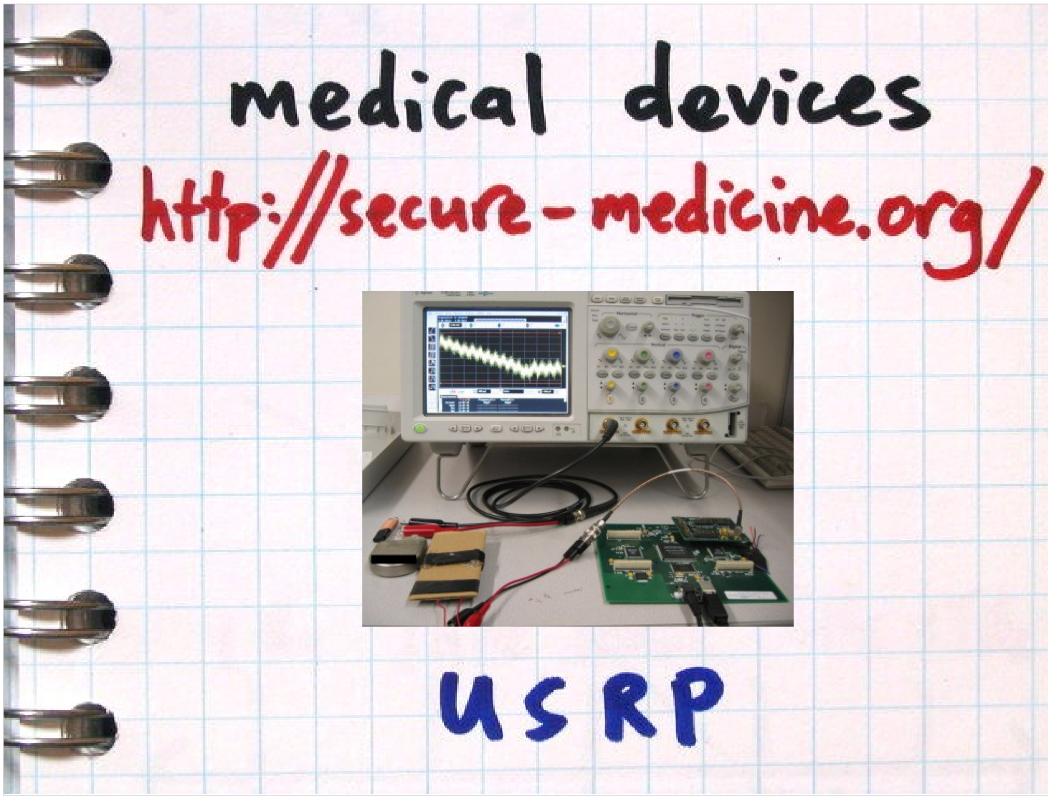
http://events.ccc.de/congress/2006/Fahrplan/events/1576.en.html

USRP/GNU Radio
decoded low frequency RFID signals
iPod replay



mobitex
http://www.toolcrypt.org/

sound card with RF front end
decoded mobitex signals

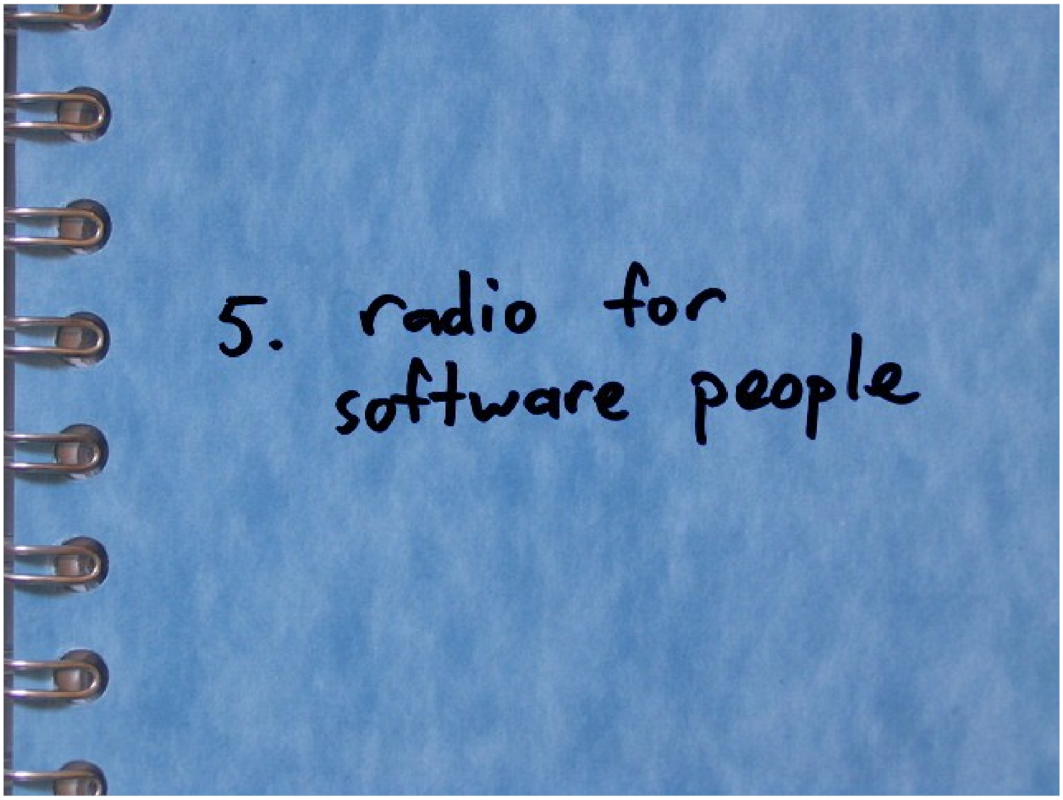


medical devices

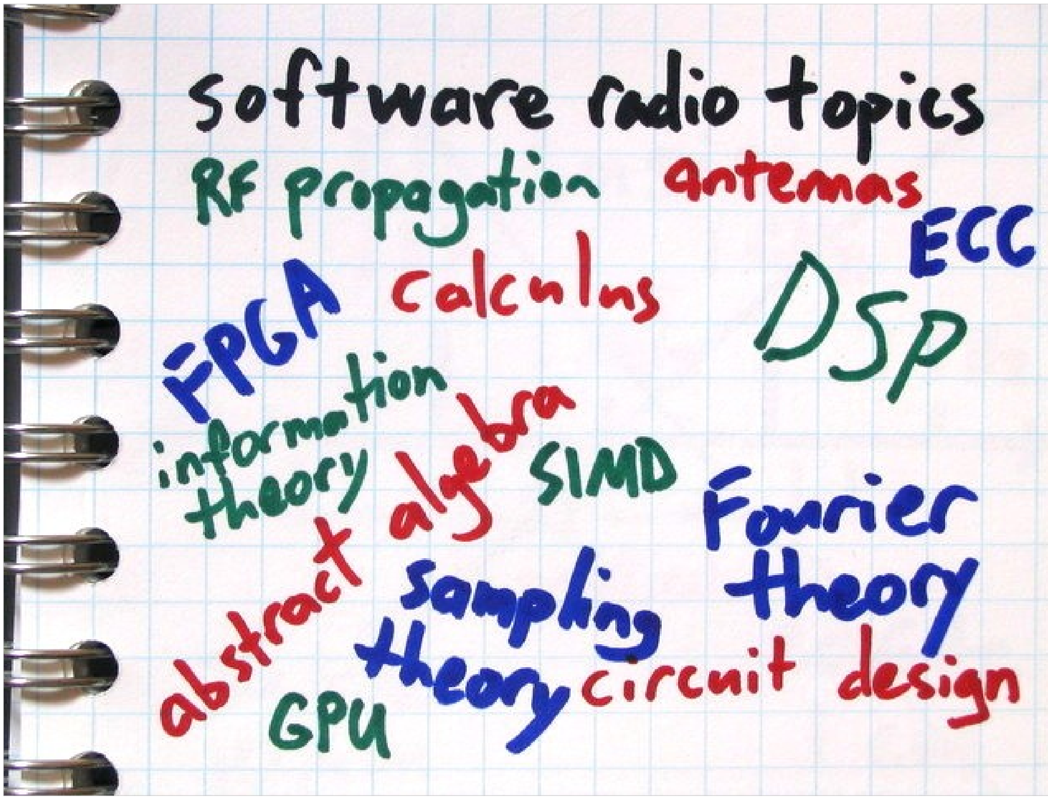
http://www.secure-medicine.org/icd-study/icd-study.pdf

- USRP/GNU Radio
- active and passive attacks against implantable cardioverter defibrillators

4. demonstration

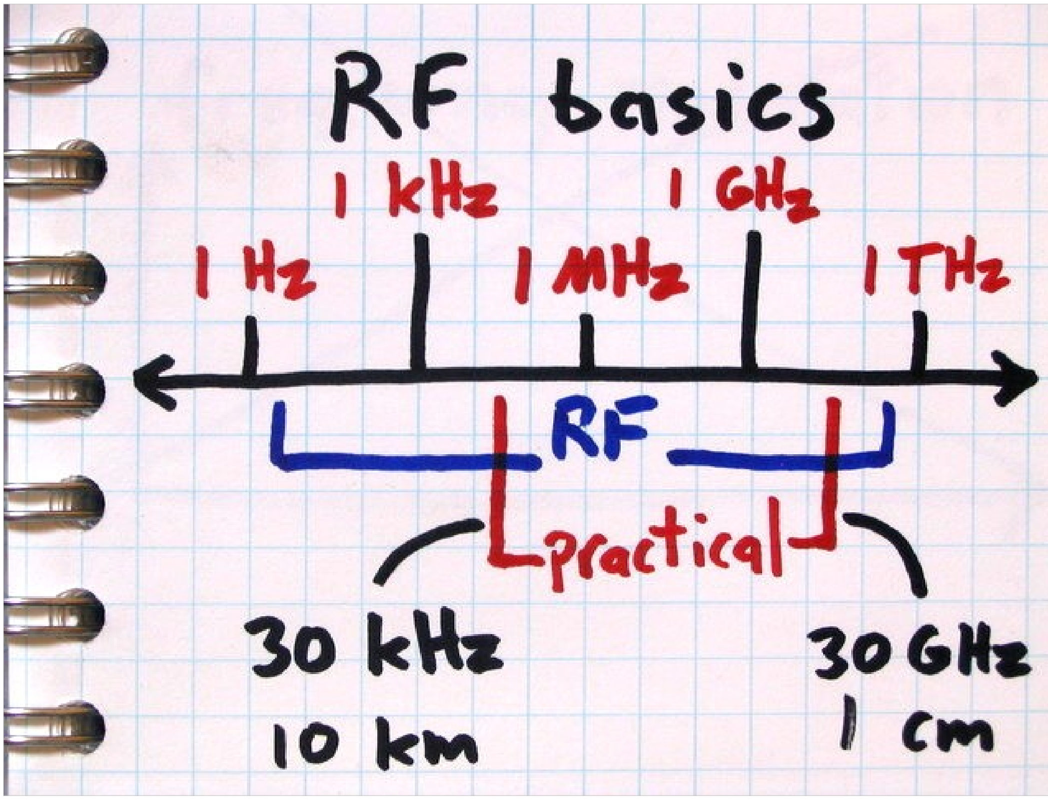


5. radio for software people



software radio topics

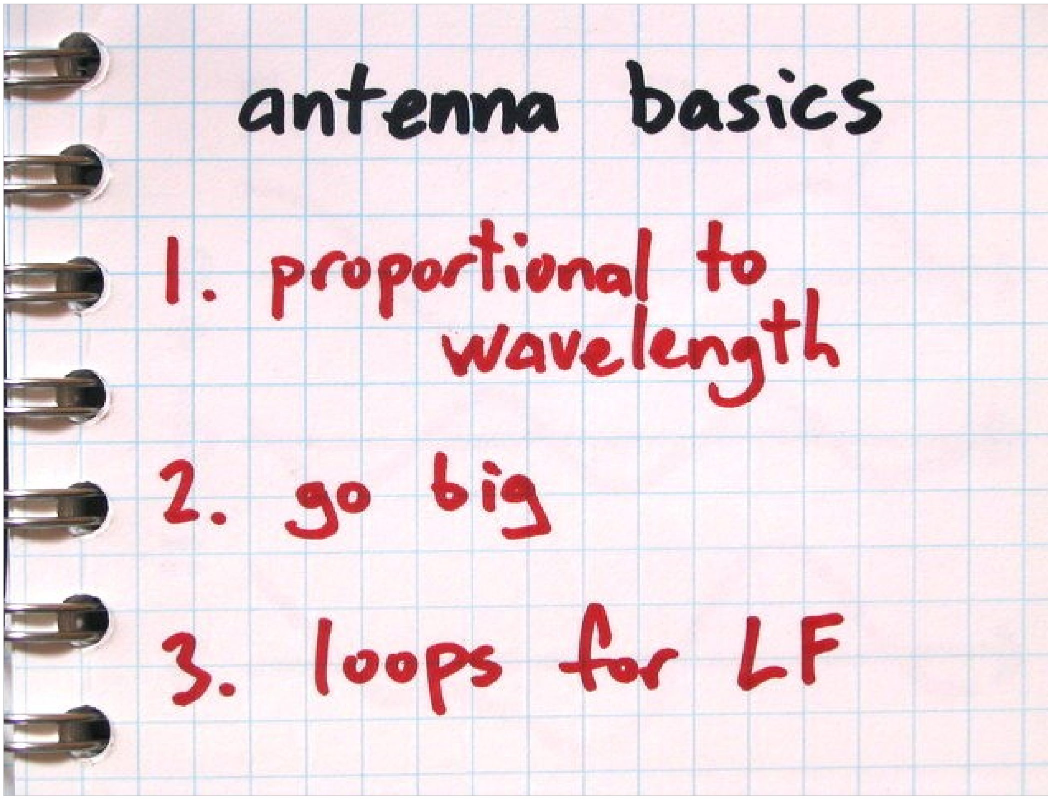
- Fortunately only a small subset of this knowledge is required to get started using software radio for useful security tasks:



RF basics

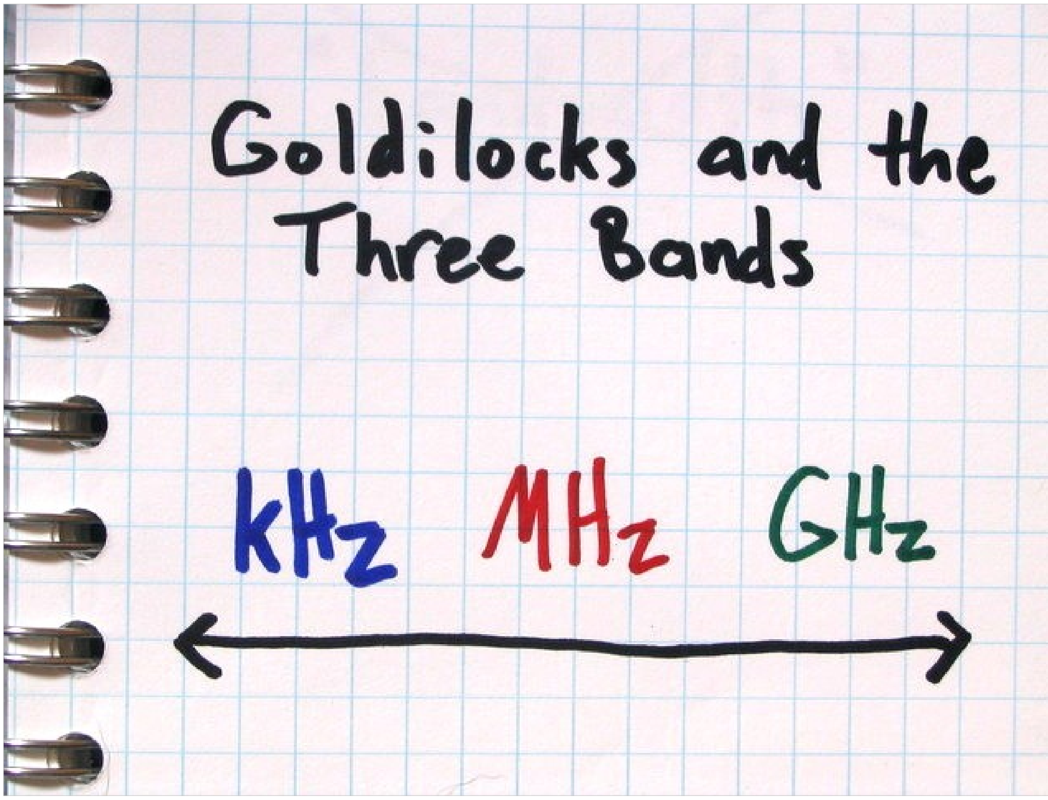
radio waves are electromagnetic radiation in the range of about 3 Hz to 300 GHz (wavelengths of 100,000 km to 1 mm)

most practical applications are between 30 kHz and 30 GHz (wavelengths of 10 km to 1 cm)



antenna basics

most jobs don't require an optimal antenna
longer wavelengths require bigger antennas
it's better to go too big than too small
low frequency applications (like 125 kHz or 134 kHz RFID tags) require loops

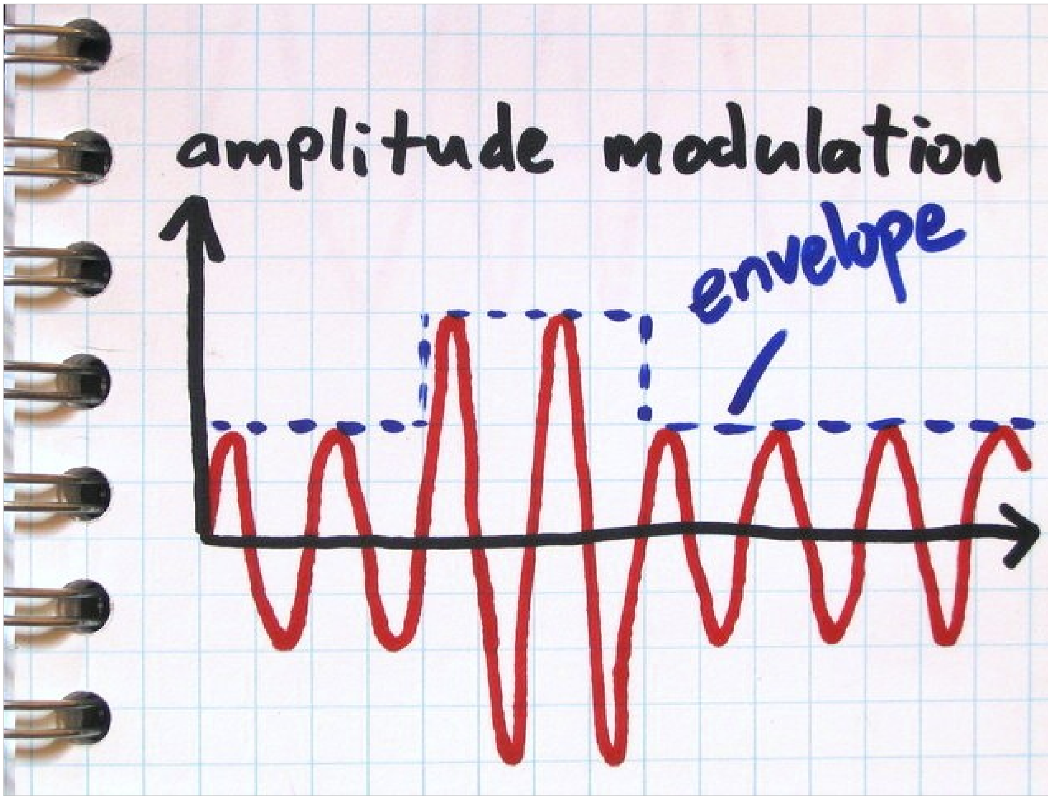


Goldilocks and the Three Bands

kHz: These wavelengths are too long!
- antennas are unwieldy
- bandwidth is limited

GHz: These wavelengths are too short!
- propagation is poor
- short range, LOS, or directional applications only

MHz: These wavelengths are just right!
- manageable antennas
- reasonable bandwidth
- good propagation

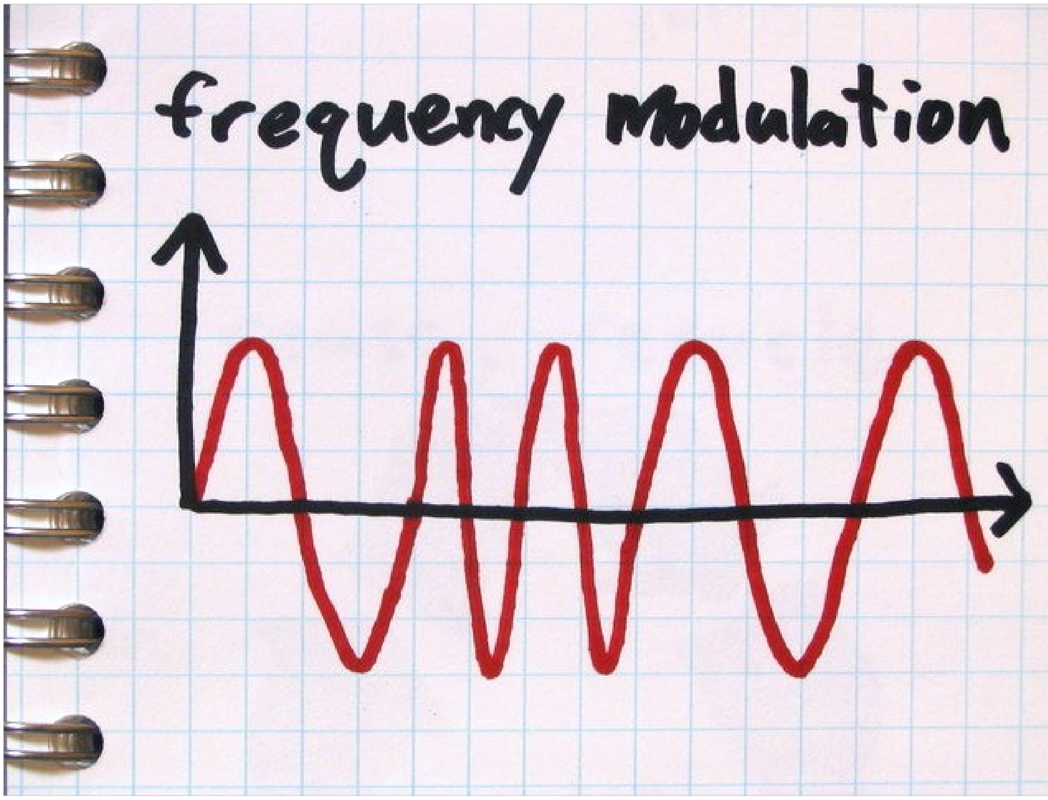


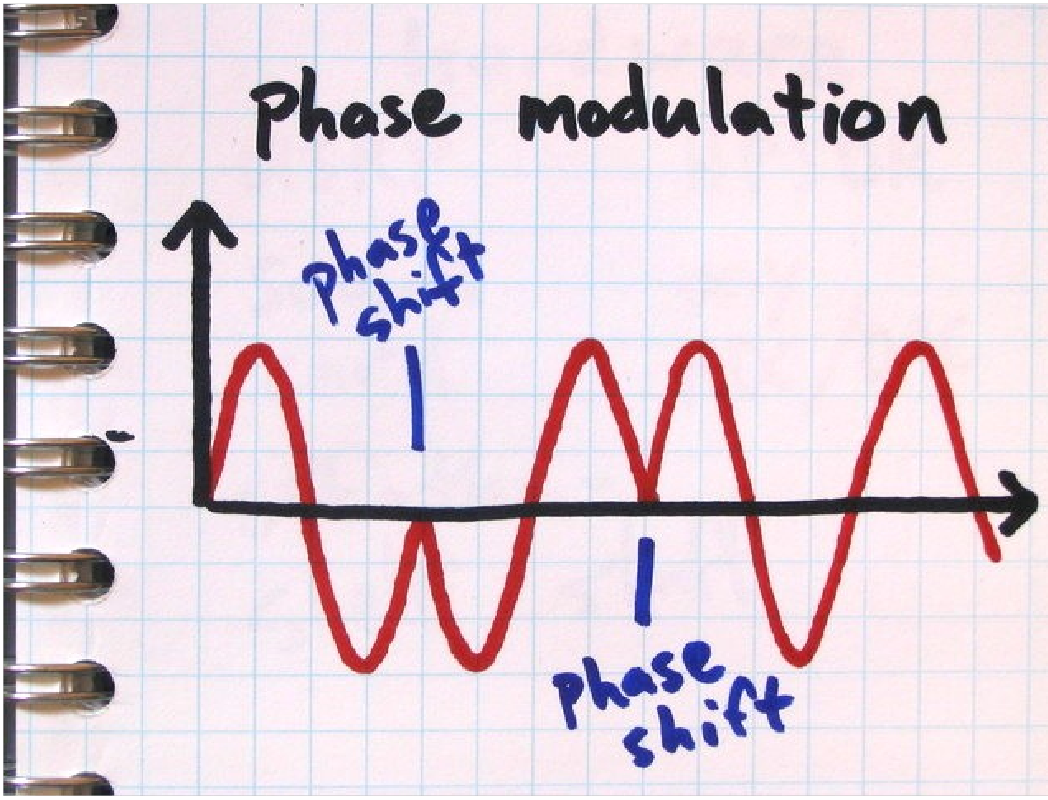
modulation

there are only three basic types of modulation:
- amplitude modulation
- frequency modulation
- phase modulation

there are many combinations and variations of these three

digital modulations are often referred to as “keying”


frequency modulation

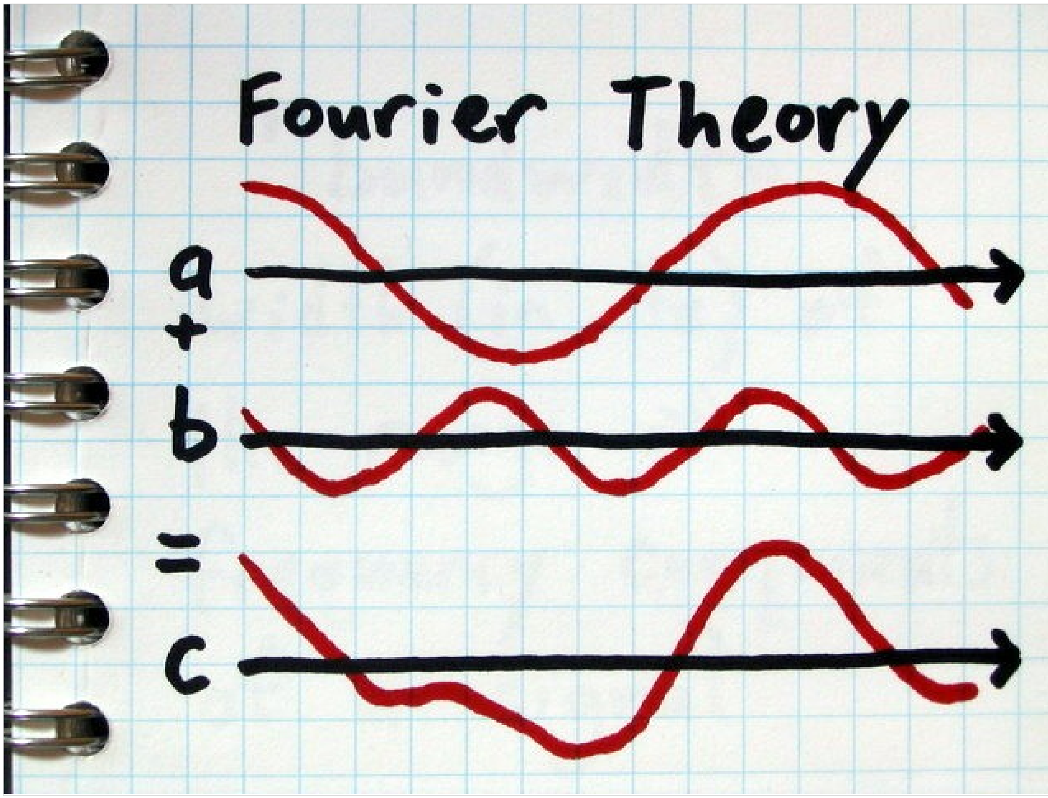


symbols

a symbol is the shortest segment of a signal that represents a discrete value of the digital data being transmitted

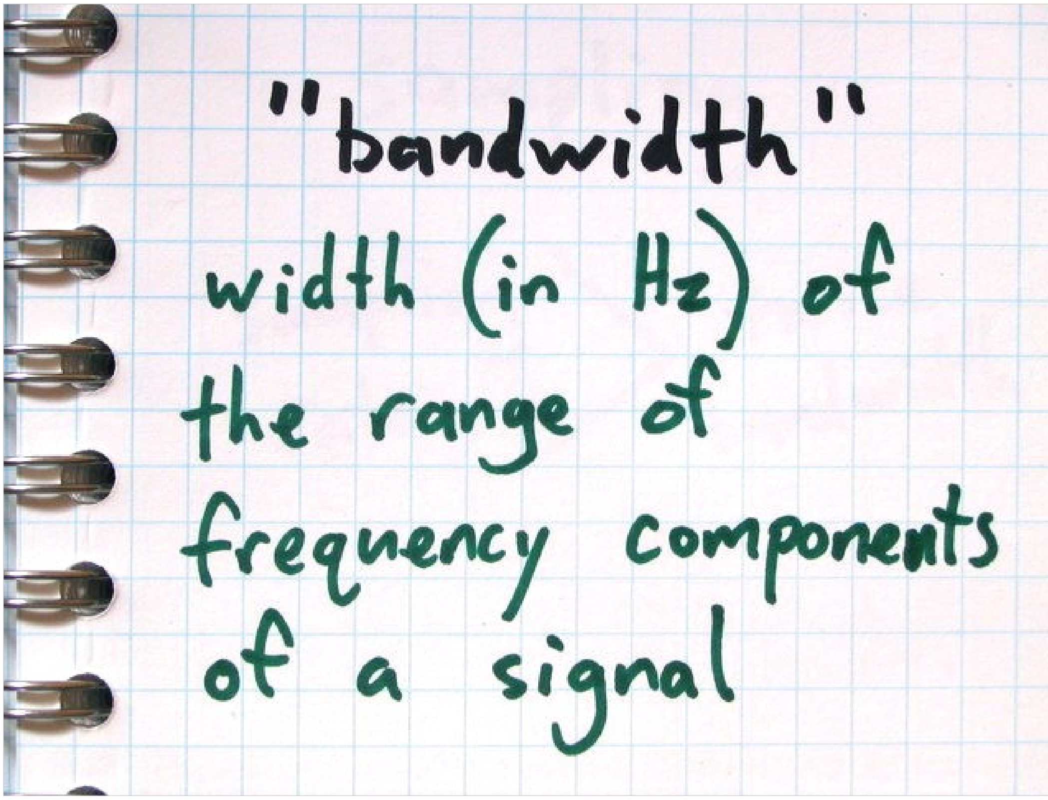
example: Binary Frequency Shift Keying (BFSK) uses one frequency for “0” and another for “1”

the symbol rate (or “baud rate”) is the number of symbols transmitted per second



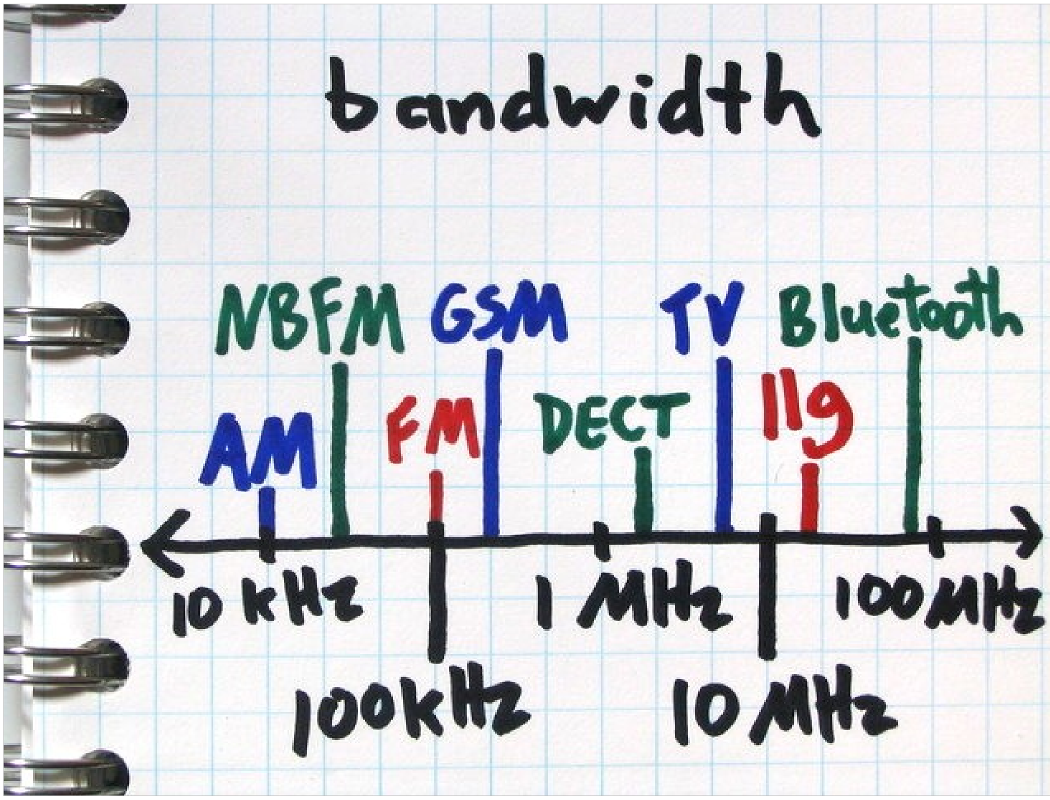
remember the Fourier transform?

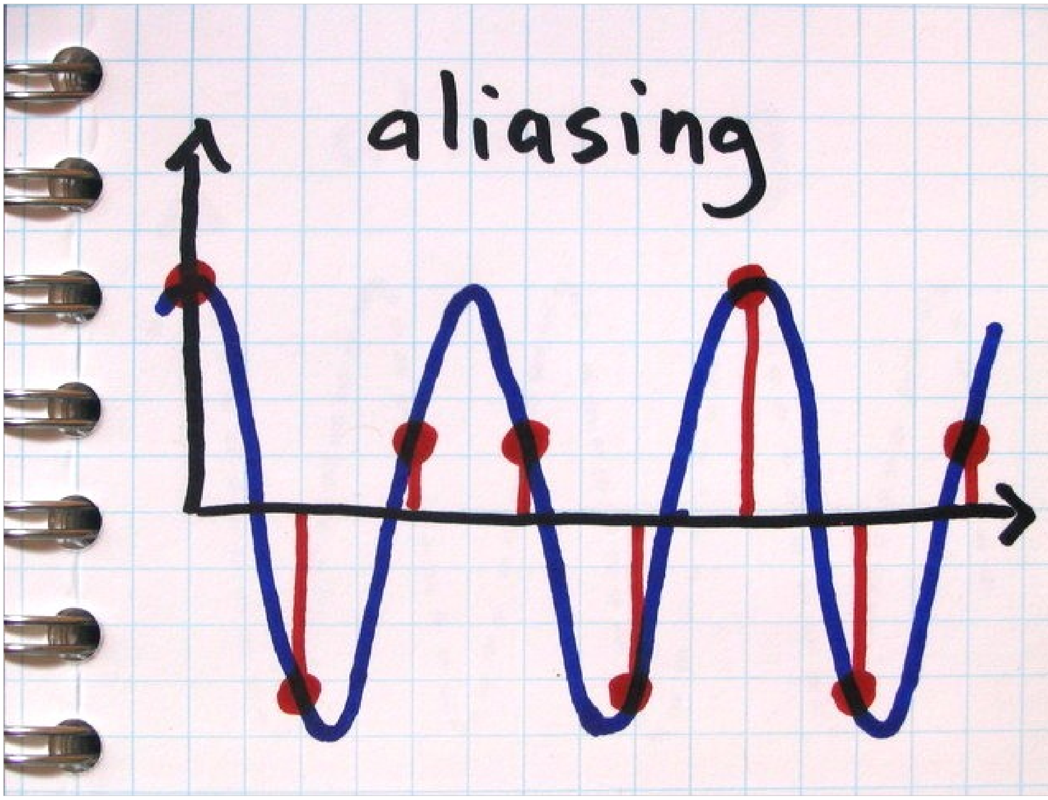
taught in Calculus courses
essential for DSP
important principle: any waveform can be precisely represented as a sum of sinusoidal components
Fast Fourier Transform (FFT) is the common digital equivalent
invertible function



“bandwidth”

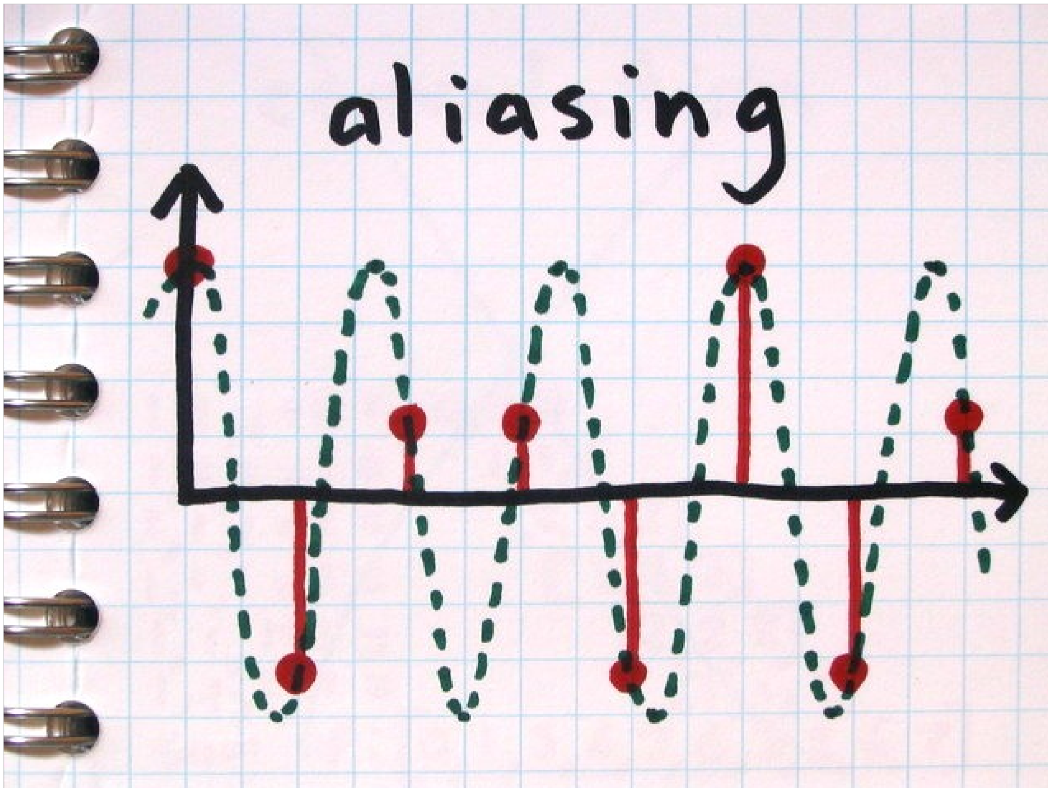
- the word “bandwidth” is overloaded but has a particular meaning in the RF/DSP world:
  - the width (in Hz) of the range of frequency components of a signal
- wider bandwidth signals have greater channel capacity (they can carry more bits per second)
- spread spectrum technologies intentionally squander channel capacity in exchange for resistance to interference

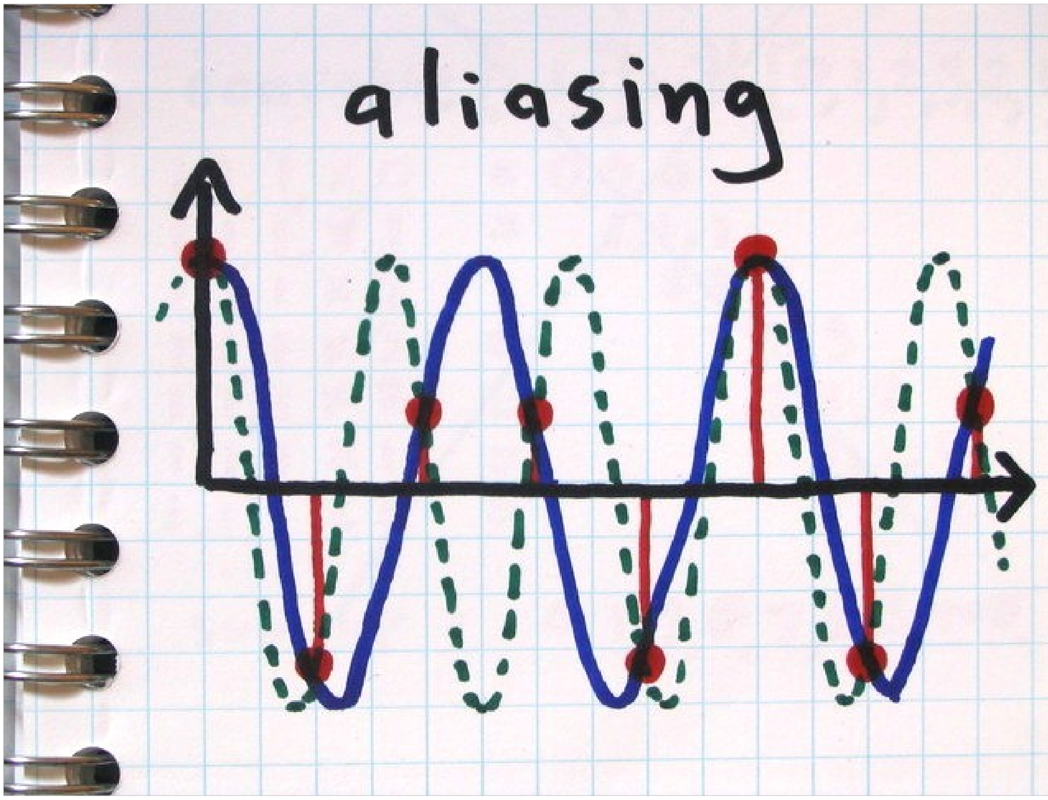

bandwidth
NBFM
GSM
TV
Bluetooth
AM
FM
DECT
11g
10 kHz
1 MHz
100 MHz
100 kHz
10 MHz

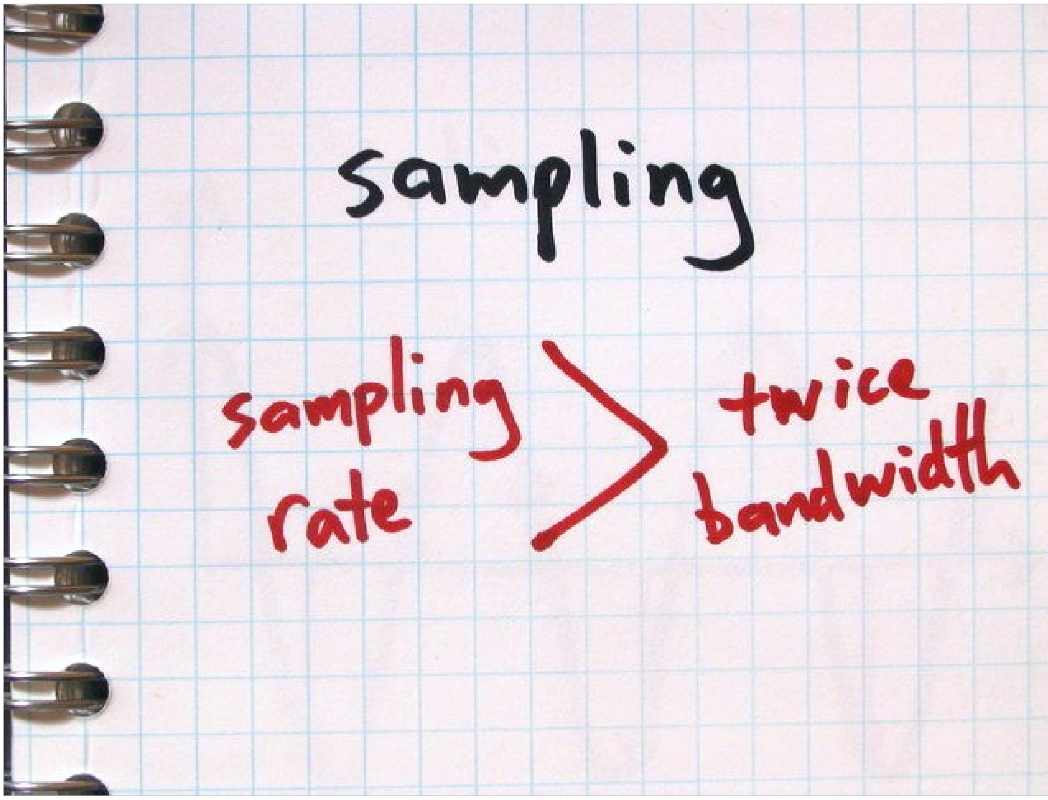


aliasing

- frequency components of sampled signals are ambiguous
- example: a 150 kHz sinusoid sampled at 192 ksps is indistinguishable from a 234 kHz sinusoid sampled at 192 ksps (both are 42 kHz away from the sample rate)
- anti-aliasing filters must be present in the analog domain


aliasing

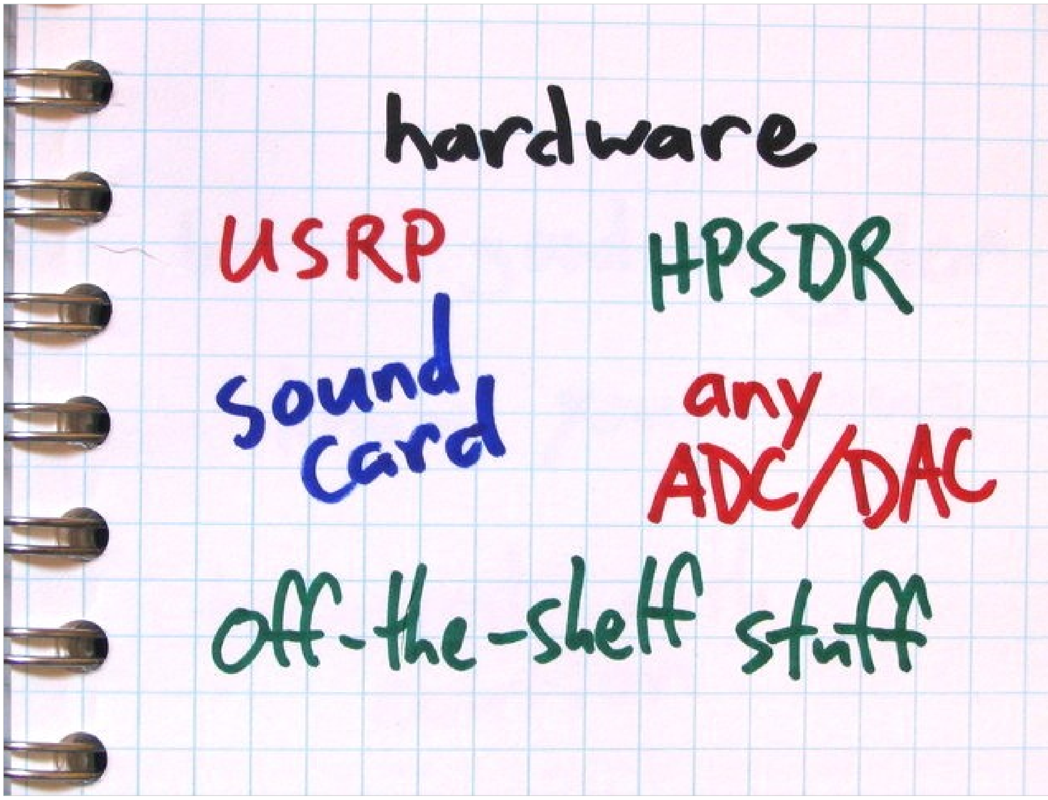

aliasing



sampling theory

in order to capture a signal, your sampling rate must be at least twice the bandwidth of the signal

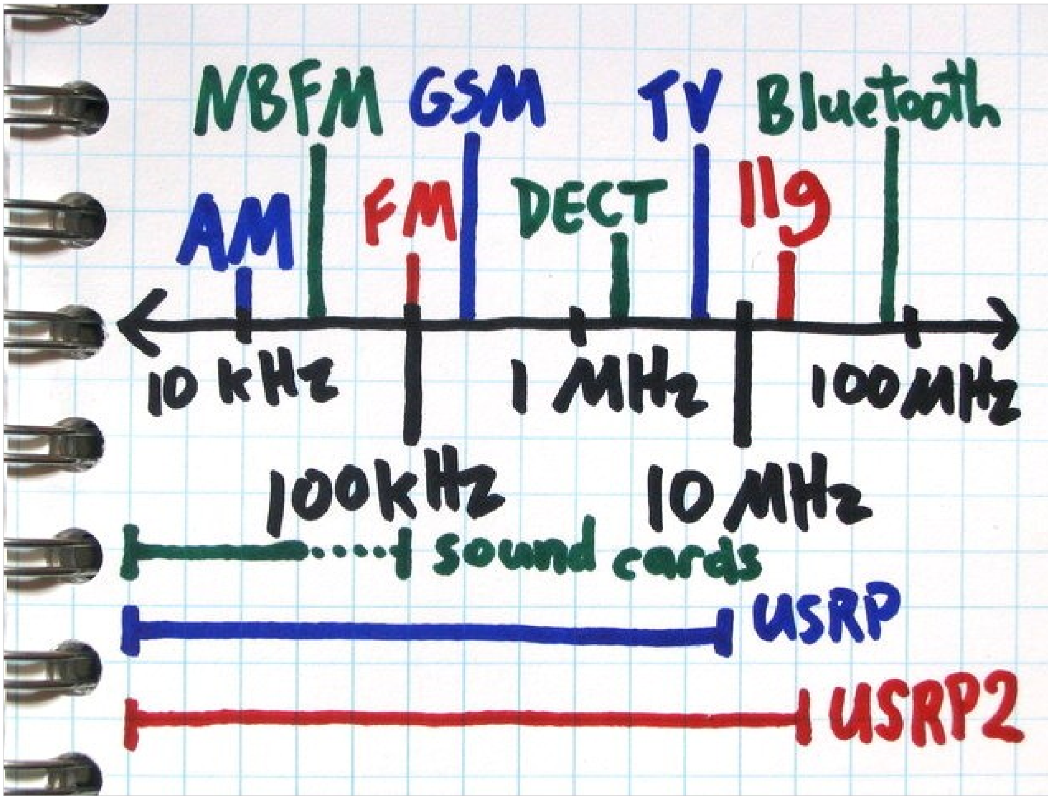
example: to capture a 25 kHz wide analog FM transmission, your ADC must acquire no less than 50,000 samples per second



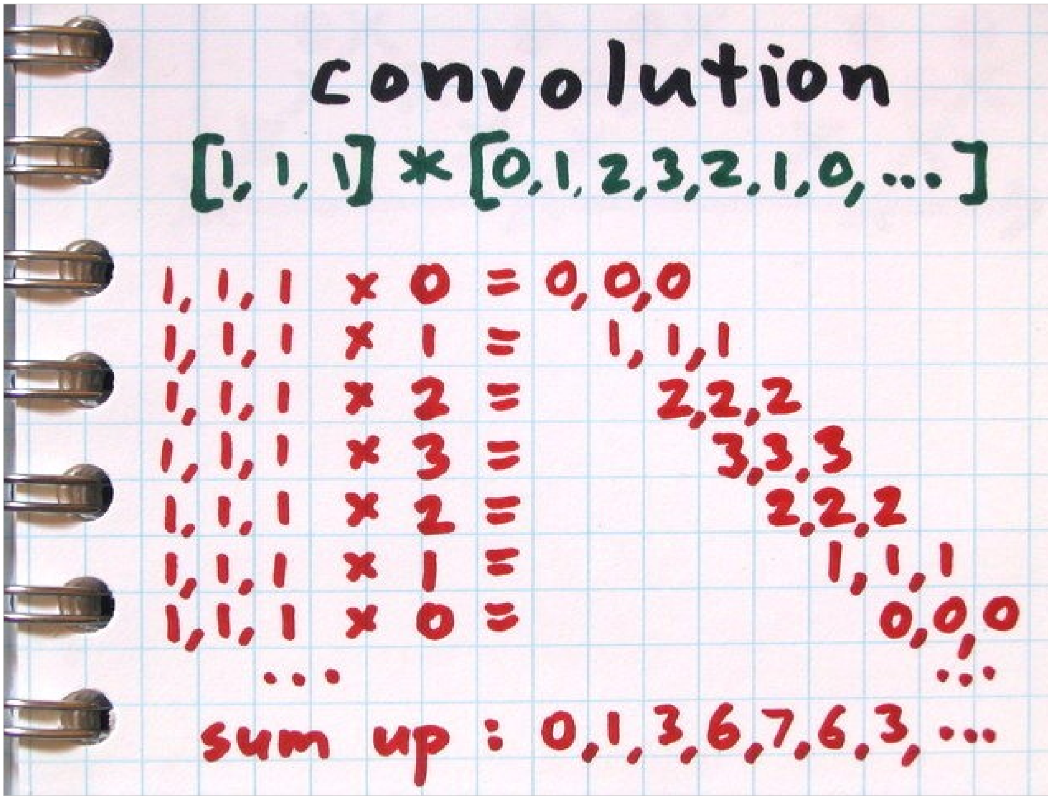
hardware options

USRP
HPSDR
sound card with RF front end
anything with ADC/DAC
- DAQ boards
- TV tuners
- video cards

hack off-the-shelf software radio equipment
you can even get started without hardware!



NBFM
GSM
TV
Bluetooth
AM
FM
DECT
11g
10 kHz
1 MHz
100 MHz
100kHz
10 MHz
sound cards
USRP
USRP2

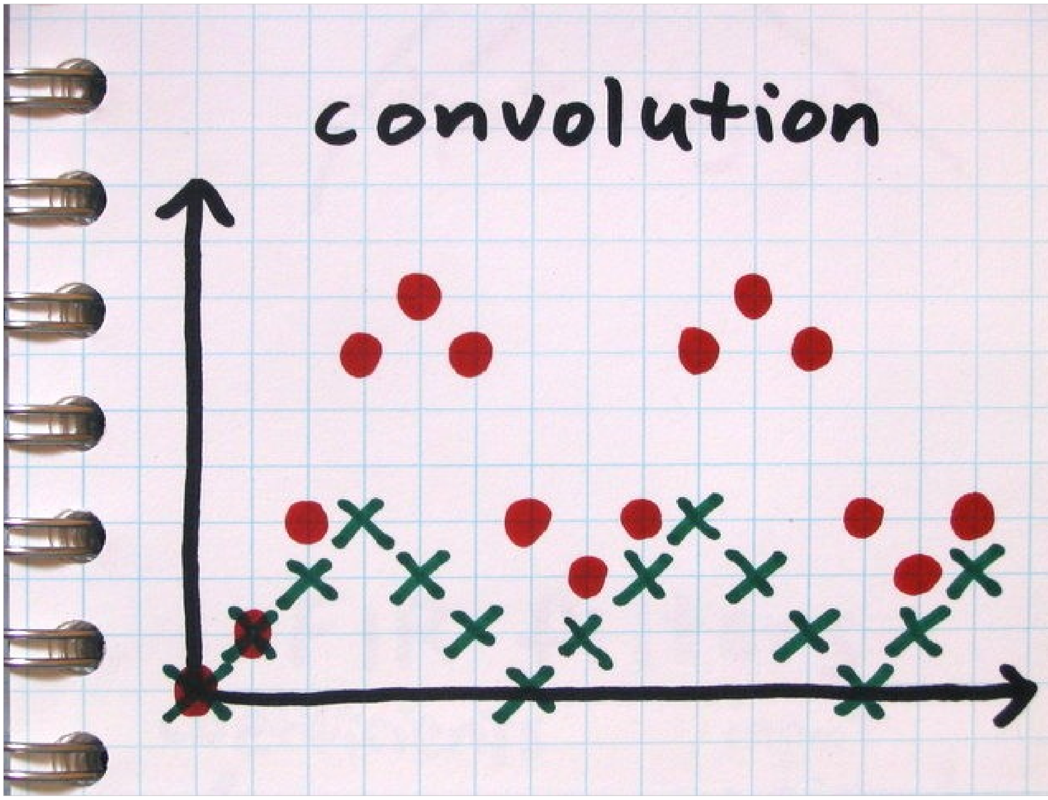


convolution

a simple and useful operation best illustrated by example:

convolve [1,1,1] with [0,1,2,3,2,1,0,1,2,3,2,1]:

```
[1,1,1] * 0 = [0,0,0]
[1,1,1] * 1 =   [1,1,1]
[1,1,1] * 2 =     [2,2,2]
[1,1,1] * 3 =       [3,3,3]
[1,1,1] * 2 =         [2,2,2]
...
sum up:       [0,1,3,6,7,6,3,2,3,6,7,6,3,1]
```



convolution as a filter

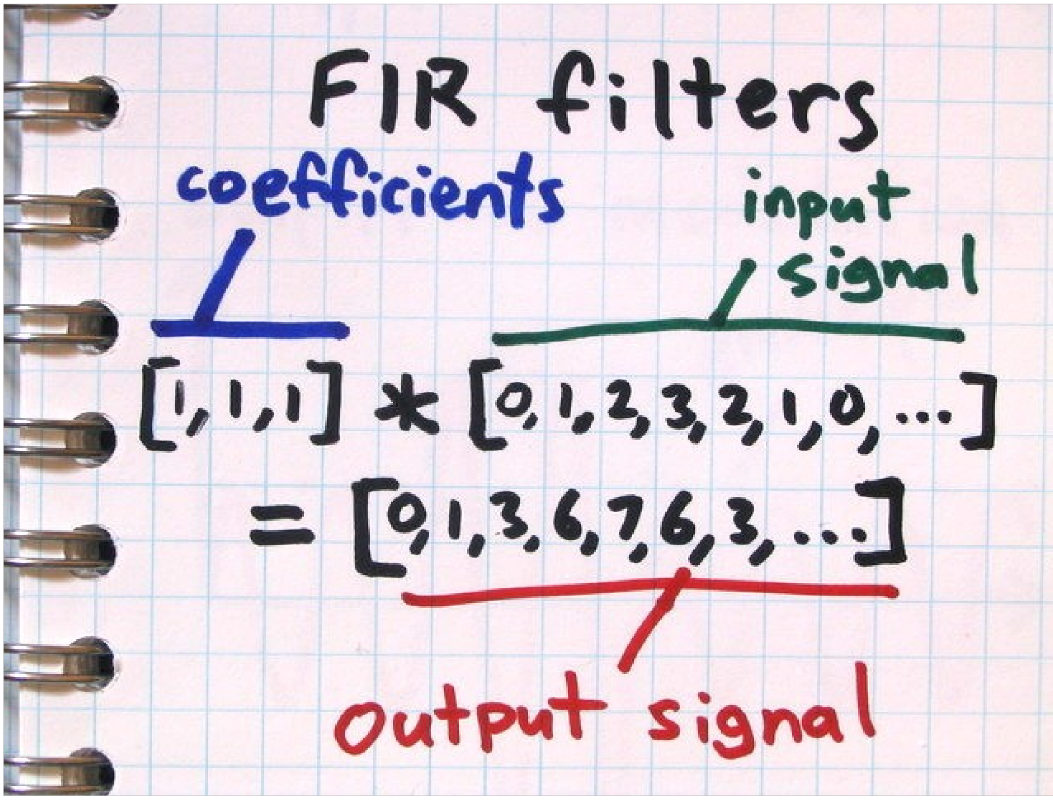
The convolution of [1,1,1] with [0,1,2,3,2,1,0,1,2,3,2,1] is a moving average and can be thought of as a filter:

[0,1,2,3,2,1,0,1,2,3,2,1] is the signal

[1,1,1] is a crude low pass filter

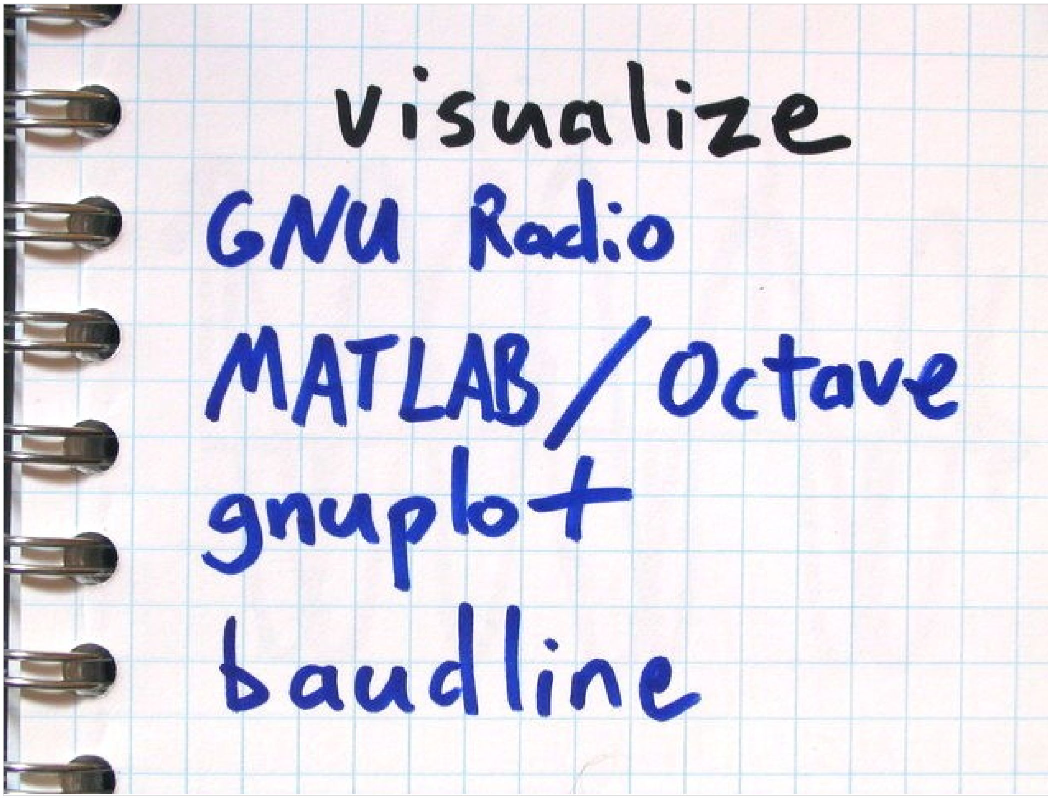
“low pass” means that it filters out high frequency components but allows the low ones to pass through

low pass filters result in smoother, rounder, waveforms



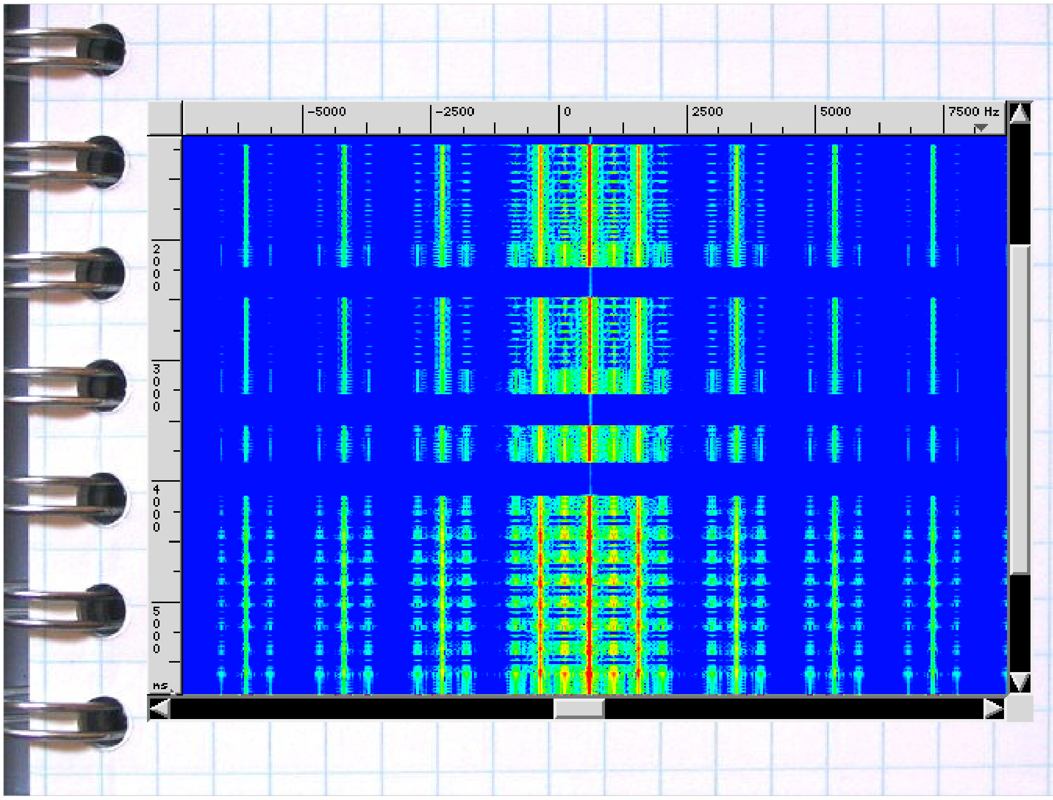
FIR filters

convolution of a signal with a static sequence is called a Finite Impulse Response (FIR) filter
the elements of the static sequence are called the coefficients of the filter
FIR filters can be used to emphasize arbitrary frequency components or remove others
High pass, low pass, and band pass are common, but more complex shapes are possible
FIR filters can be fast (SIMD, DSP chips, etc.)
common routines are available to “design” (produce the coefficients for) filters based on the required shape in the frequency domain (the filter's “frequency response”)
always test filters



visualize, visualize, visualize

GNU radio
gnuplot
various audio tools
my favorite: baudline (free but closed source)

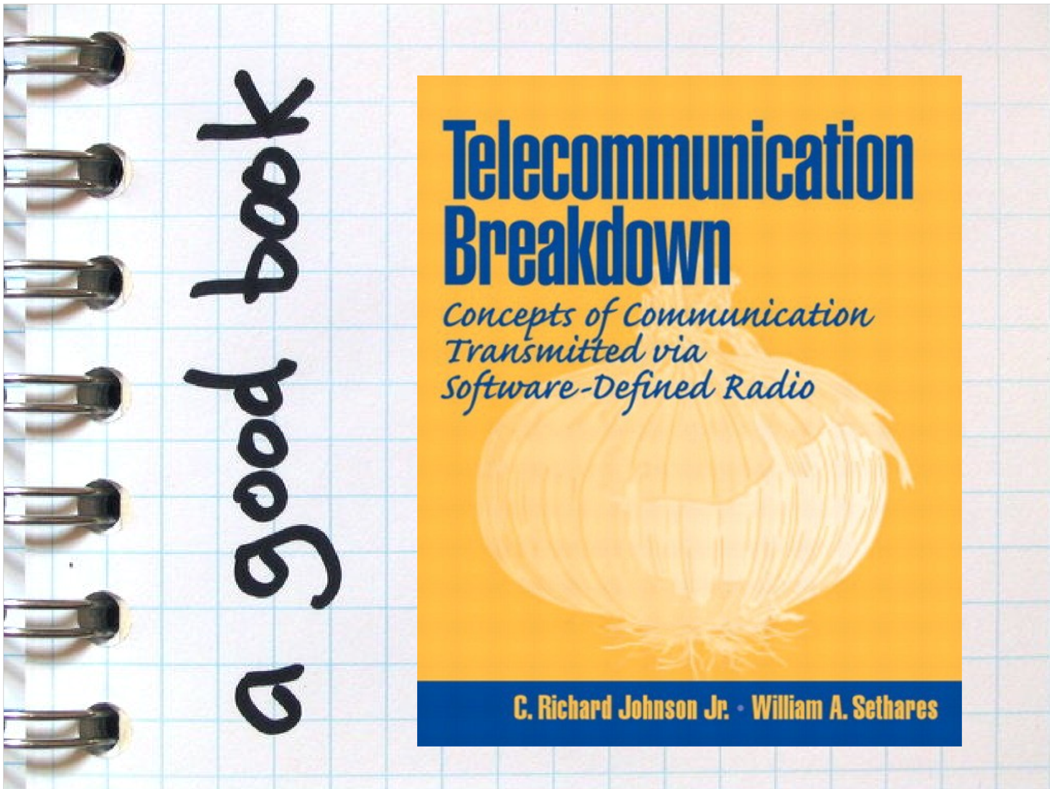


-5000
-2500
0
2500
5000
7500 Hz
2000
3000
4000
5000
ms

software re-use

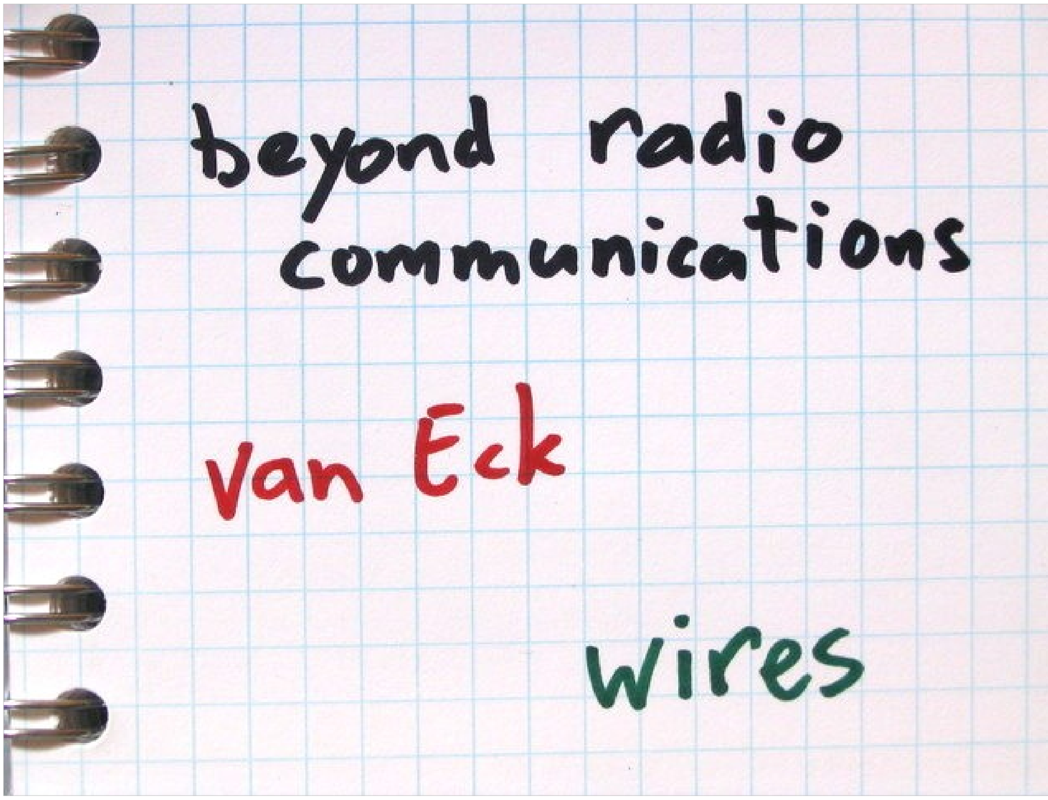
GNU Radio and other frameworks include code for:

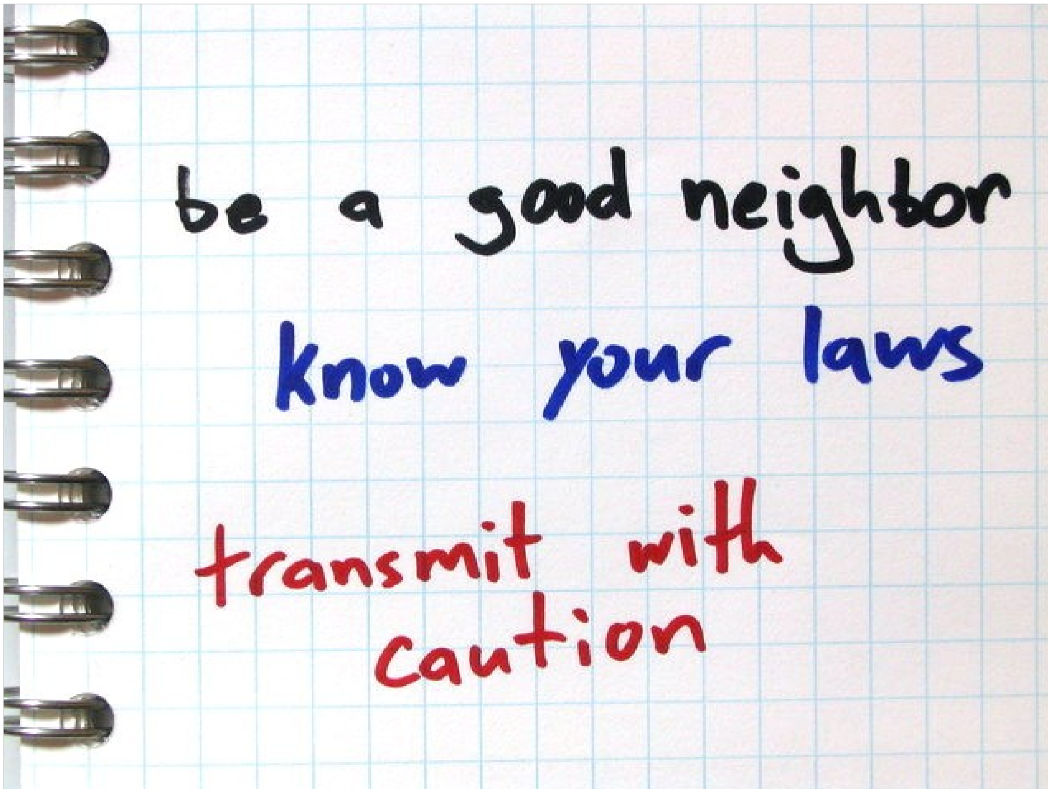
- filters
- filter design functions
- resampling
- frequency conversion
- modulation
- demodulation
- and much more



a good book

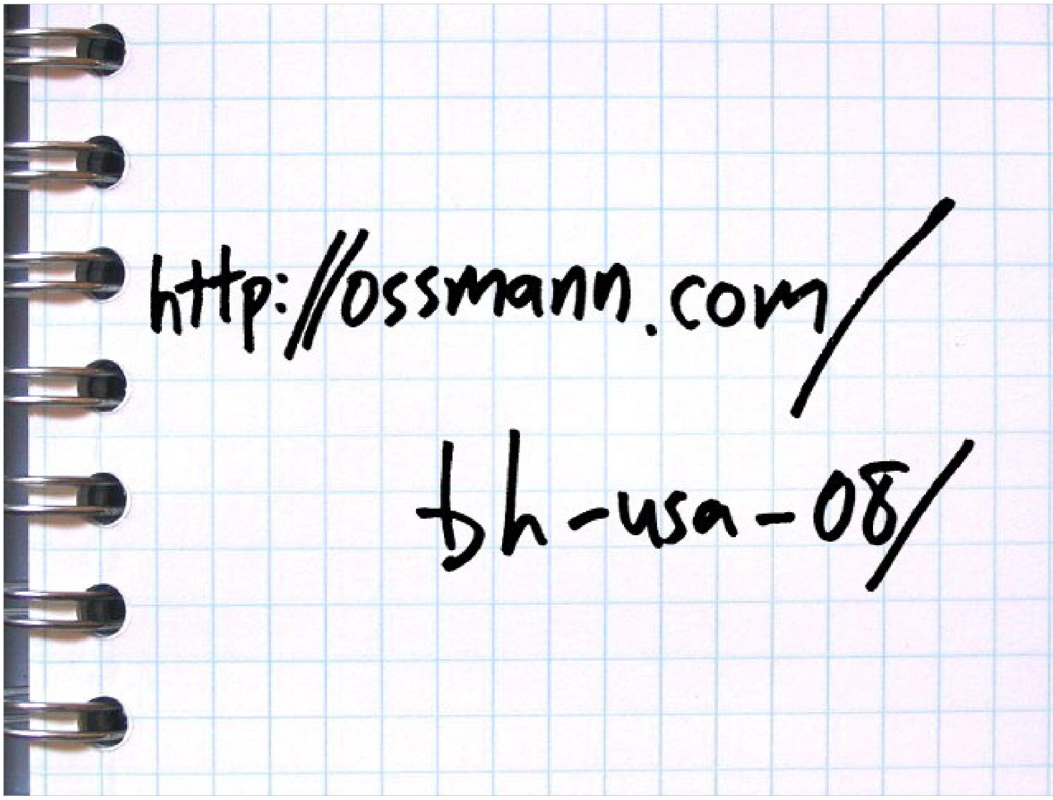
http://eceserv0.ece.wisc.edu/~sethares/telebreak.html


beyond radio
communications
van Eck
wires



be a good neighbor

- know your laws
- don't transmit anything over the air without being sure of what you are doing
  - you can often use cables instead (but don't forget attenuators)
- common transmission mistakes:
  - failure to filter noise outside of the intended signal bandwidth
  - failure to filter aliases


http://ossmann.com/
bh-usa-08/

C. R. Johnson, Jr. and W. A. Sethares. Telecommunication Breakdown: Concepts of Communication Transmitted via Software-Defined Radio.
http://eceserv0.ece.wisc.edu/~sethares/telebreak.html

The GSM Software Project
http://wiki.thc.org/gsm

Max Moser and Phill Schrödel. 27Mhz based wireless security insecurities.
http://www.remote-exploit.org/advisories.html

Dominic Spill and Andrea Bittau. BlueSniff: Eve meets Alice and Bluetooth.
http://www.usenix.org/event/woot07/tech/full_papers/spill/

Henryk Plötz. RFID Hacking.

http://events.ccc.de/congress/2006/Fahrplan/events/1576.en.html

olleB. Mobitex Network Security.
http://cansecwest.com/csw08/csw08-olleb.pdf
http://www.toolcrypt.org/

Daniel Halperin, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.
http://www.secure-medicine.org/icd-study/icd-study.pdf

GNU Radio: the gnu software radio.
http://gnuradio.org/trac

The Universal Software Radio Peripheral (USRP).
http://www.ettus.com/

High Performance Software Defined Radio.

http://hpsdr.org/

baudline signal analyzer.

http://www.baudline.com/

MATLAB.

http://www.mathworks.com/

GNU Octave.

http://www.gnu.org/software/octave/

OP25. A software-defined analyzer for APCO P25 signals.

http://sedition.org.au/op25